(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号
特表2001－518255
（P2001－518255A）
(43)公表日　平成13年10月９日(2001.10.9)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｇ０６Ｋ　17/00		Ｌ
Ｇ０６Ｋ　17/00				Ｎ
		Ｇ０９Ｃ　1/00		６６０Ａ
19/00		Ｈ０４Ｈ　1/00		Ｆ
19/07		Ｈ０４Ｎ　7/167		Ｚ

審査請求　未請求　予備審査請求　有　（全 78 頁）　最終頁に続く

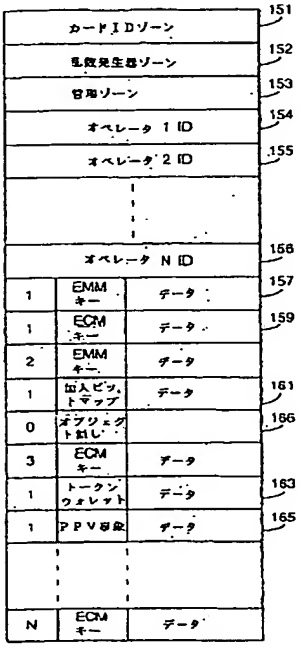
(21)出願番号　特願平10－542063
(86)（22)出願日　平成９年４月25日(1997.4.25)
(85)翻訳文提出日　平成11年９月17日(1999.9.17)
(86)国際出願番号　ＰＣＴ／ＥＰ９７／０２１０７
(87)国際公開番号　ＷＯ９８／４３４２５
(87)国際公開日　平成10年10月１日(1998.10.1)
(31)優先権主張番号　９７４００６５０．４
(32)優先日　平成９年３月21日(1997.3.21)
(33)優先権主張国　ヨーロッパ特許庁（ＥＰ）

(71)出願人　カナル　プラス　ソシエテ　アノニム
フランス国　エフ－75711　パリ　セデックス　15　クアイ　アンドレ　シトロエン　85／89
(72)発明者　メイラード，マイケル
フランス国　エフ－28120　マインテノン　アベニュ　デュ　マレシャル　レセル　42
(72)発明者　ベナルドゥー，クリスチアン
フランス国　エフ－77600　ビュジー　サン　ジョルジ　アレ　デ　ピュイザチュエ　13
(74)代理人　弁理士　斉藤　武彦　（外１名）
最終頁に続く

(54)【発明の名称】　暗号化放送信号の受信機と併用するためのスマートカード、および受信機

(57)【要約】
暗号化放送信号の受信機と併用するためのスマートカードは、前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサを備えている。メモリがマイクロプロセッサに結合されている。このマイクロプロセッサは、メモリのそれぞれの動的に作成されたゾーンによってこのような信号のそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、動的に作成されたゾーンの各々は前記放送供給者のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成されている。

Fig.19.



【特許請求の範囲】

１．暗号化放送信号の受信機と併用するためのスマートカードであって、

前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、

前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサが、前記メモリ内の各々の動的に作成されたゾーンからなる手段によってこのような信号に付いてのそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、且つ前記動的に作成されたゾーンは各々が前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成されていることを特徴とするスマートカード。

２．前記放送供給者の中のそれぞれの放送供給者に関連した識別子および少なくとも１つの秘密暗号解読キーをさらに備え、前記識別子および前記キーキーが、前記動的に作成されたゾーンの中の１つに記憶され、かつこの識別子に対応するＩＤを有し且つ、この暗号解読キーに対応する暗号化キーを使用して暗号化された放送信号を暗号解読するように構成され、ることを特徴とする請求項１に記載のスマートカード。

３．各ゾーンに対して記憶されたグループ識別子と、このグループ内部のグループ識別子を識別し、前記記憶されたグループ識別子に対応するＩＤを有する放送信号を暗号解読するように構成された他の識別子とをさらに備えていることを特徴とする請求項２に記載のスマートカード。

４．それぞれの放送供給者のＩＤを含むメモリゾーンに於ける第１のシリーズ及び動的に作成されたメモリゾーンに於ける第２のシリーズとを保持するように構成され、前記第２のシリーズに於けるメモリゾーンの各々は、放送供給者のＩＤを示すラベルを付けられ、この供給者からの受信放送信号の処理のために使用される前記暗号解読データを含むデータ含み、第２のシリーズに於ける複数のメモリゾーンは、共通ＩＤラベルを有し、この放送供給者からの受信放送信号の処理に関する異なる種類のデータを含むことを特徴とする前述の請求項１乃至３のいずれかに記載のスマートカード。

５．前記スマートカードが前記第１のシリーズのメモリゾーンを動的に作成するように構成されていることを特徴とする請求項４に記載のスマートカード。

６．前記動的に作成されたメモリゾーンが連続的であることを特徴とする前述の請求項１乃至５のいずれかに記載のスマートカード。

７．前記動的に作成されたゾーンの動的作成を制御するデータを記憶するように構成された管理メモリゾーンをさらに備えていることを特徴とする前述の請求項１乃至６のいずれかに記載のスマートカード。

８．一つの前記動的に作成されたゾーンが、放送供給者によって放送された放送項目の中から特定の項目を選択を示す権利データを含み、前記スマートカードの使用者暗号を解読する為の権利を有し、且つ当該スマートカードは、この供給者によって放送された項目を暗号解読するように権利データを使用する様に構成されていることを特徴とする前述の請求項１乃至７のいずれかに記載のスマートカード。

９．トランザクションメモリゾーンが、前記動的に作成されたゾーンに加えて前記スマートカードに規定され、かつ前記スマートカードのユーザが、前記ユーザの制御の下で前記スマートカードによって発生することができるトランザクション出力信号に応じてのみ暗号解読する権利が付与されている放送供給者によって放送された項目に関する他の権利データを含んでいることを特徴とするいずれかの前述の請求項に記載のスマートカード。

１０．ある項目が前記トランザクション出力信号の出力に続いて放送される機会の数を計数するカウンタをさらに備え、かつ前記スマートカードが、前記カウンタによって到達された計数値に応じてこの項目の暗号解読を制御するように構成されている請求項９に記載のスマートカード。

１１．前記受信機／デコーダが、スマートカード読み取り器を備え、かつ当該スマートカード読み取り器は、前記加入者スマートカードの制御の下で放送暗号化信号を暗号解読するように構成されていることを特徴とする前述の請求項１乃至１０のいずれかのに記載のスマートカードと併用するための受信機／デコーダ。

１２．前記受信機／デコーダが暗号化放送ビデオおよび／またはオーディオ信号

を暗号解読し、かつ対応するビデオおよび／またはオーディオ出力を発生するように構成されている請求項１１に記載の受信機／デコーダ。

１３．前記受信機／デコーダが前記暗号化放送信号を受信する比較的高いバンド幅入力ポートと、前記出力制御信号を放送送信機に送り返すように構成された比較的低いバンド幅出力ポートとを有することを特徴とする請求項１１あるいは１２に記載の受信機／デコーダ。

１４．前記受信機／デコーダが、記憶された識別子を含み、かつ対応する記憶された識別子を有するスマートカードとだけ作動するように構成された請求項１１～１３のいずれかに記載の受信機／デコーダ。

１５．暗号化信号を受信機／デコーダに放送する装置であって、前記装置が、２又はそれ以上の種類の放送制御信号を発生する手段を備え、当該制御信号の各種類が、対応するＩＤを有する受信機／デコーダをこのような種類の制御信号に対して選択的に応答するようにした受信機／デコーダＩＤデータを含み、前記受信機／デコーダＩＤデータの１つあるいはそれ以上のグループの受信／デコーダの全てが、共通の種類の制御信号に応答するように構成されたグループＩＤデータを含み、前記装置には、入力情報に応じて異なるＩＤグループ間に個別の受信機／デコーダを動的に分配するように構成されているデータベース手段が装備されていることを特徴とする装置。

１６．前記データベース手段が、前記受信機／デコーダから受信された信号に応答し、グループ間の受信機／デコーダの分配を変えることを特徴とする請求項１５に記載の装置。

１７．前記装置が、前記入力情報に応じてグループ間の受信機／デコーダの分配を変える制御信号を放送するように構成されたことを特徴とする請求項１５あるいは請求項１６に記載の装置。

１８．制御信号の異なる種類が、放送暗号化データストリームの異なる部分の暗号解読を可能にすることを特徴とする請求項１５～１７のいずれかに記載の装置。

１９．前記入力情報が支払い情報を含むことを特徴とする請求項１５～１８のいずかに記載の装置。

２０．制御信号の当該種類が異なる放送供給者からの暗号化放送信号を暗号解読する加入操作を制御する種類を含むことを特徴とする請求項２０あるいは請求項２１に記載の装置。

２１．制御信号の種類が、異なる時間フレームに於ける放送暗号化データ信号を暗号解読する権利の購入を制御する種類を含むことを特徴とする請求項２０あるいは請求項２１に記載の装置。

２２．前記暗号化放送信号がビデオ信号および／またはオーディオ信号であることを特徴とする請求項１５～２１のいずれかに記載の装置。

２３．前記グループが２５６人までのメンバーを有することを特徴とする請求項１５～２２のいずれかに記載の装置。

２４．前記装置が前記暗号化データ信号を軌道を回っている衛星に送信されるように構成されていることを特徴とする請求項１５～２３のいずれかに記載の装置。

２５．暗号化放送信号を受信する受信機／デコーダであって、前記受信機／デコーダが、グループＩＤを含み、かつ前記グループＩＤに対応するＩＤを有する放送制御信号のある種類に応答し、前記受信機／デコーダが他の制御信号に応じてそのグループＩＤを変えるように構成されていることを特徴とする受信機／デコーダ。

２６．前記他の制御信号が放送信号を含み、前記放送信号および前記暗号化放送信号が前記受信機／デコーダによって受信されるように構成されていることを特徴とする請求項２５に記載の受信機／デコーダ。

２７．前記グループＩＤが、前記受信機／デコーダに取り外しできるように挿入されたスマートカードに記録されていることを特徴とする請求項２５あるいは２６に記載の受信機／デコーダ。

２８．前記暗号化放送信号がビデオ信号および／またはオーディオ信号であることを特徴とする請求項２５～２７のいずれかに記載の装置。

２９．請求項２５～２８のいずれかに記載されるような受信機／デコーダとともに請求項１５～２４のいずれに記載の装置を備えているディジタルデータ信号を放送し、かつ受信するシステム。

３０．暗号化信号を受信機／デコーダに放送する方法であって、２つあるいはそれ以上の放送制御信号の種類を発生する工程を含み、当該信号の序番各種類は、対応するＩＤを有する受信機／デコーダを選択的に当該制御信号の種類に応答しうる様にするための、受信機／デコーダＩＤデータを含み、入力情報に応じて異なるＩＤグループ間に個別の受信機／デコーダを動的に分配することを含むことを特徴とする暗号化信号を受信機／デコーダに放送する方法。

３１．前記入力情報が、支払い情報を含み、且つ該制御信号の当該種類が、前記受信機／デコーダをして、暗号化放送ビデオおよび／またはオーディオストリームの一部を選択的に暗号解読せしめうるように構成したことを特徴とする請求項３０に記載の方法。

３２．暗号化信号を受信機／デコーダに放送する装置であって、当該装置は、前記暗号化信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段と、制御信号を前記放送信号内部でそれぞれのプログラム伝送に関連付ける手段とを備え、前記関連付け手段が、一連の同じプログラムの伝送における各伝送を識別する信号を発生する手段を備えていることを特徴とする暗号化信号を受信機／デコーダに放送する装置。

３３．当該装置は、更に、前記受信機／デコーダに於ける、暗号解読されうる前記一連の伝送数の制限を設定する信号を発生する手段をさらに備えていることを特徴とする請求項３２に記載の装置。

３４．前記装置が、受信機／デコーダからの入力信号に応じて前記制限を変更することを特徴とする請求項３３に記載の装置。

３５．前記装置が、前記ビデオおよび／またはオーディオストリームを軌道を回っている衛星に送信するように構成されている請求項３２～３４のいずれかに記載の装置。

３６．放送信号をペイ・パー・ビュー（ＰＰＶ）モードで受信し、かつ暗号解読する受信機／デコーダであって、当該受信機／デコーダは、前記放送信号内部で特定のプログラム伝送の暗号解読を可能にするかあるいは制御する制御信号を検出する手段を含み、前記制御信号が一連の同一プログラムの伝送における各伝送

を識別する情報を含むことと、前記検出手段に結合され、暗号解読されうる前記一連の伝送数を制限する手段とを備えていることを特徴とする受信機／デコーダ。

３７．前記制限手段が、前記シリーズ内の伝送の各連続視聴に応じて記憶された制限値に向けて増減されるように構成されるカウンタを備えていることを特徴とする請求項３６に記載の受信機／デコーダ。

３８．受信放送信号に応じて前記制限値を調整する手段をさらに備えていることを特徴とする請求項３７に記載の受信機／デコーダ。

３９．前記制限手段が、受信機／デコーダに取り外しできるように挿入されるスマートカードを備えていることを特徴とする請求項３６～３８のいずれかに記載の受信機／デコーダ。

４０．暗号化放送信号を受信し、かつ暗号解読する受信機／デコーダであって、

スマートカード読み取り器と、

前記スマート読み取り器に結合され、かつ前記スマートカードからの出力に応じて前記信号を暗号解読するように構成されているプロセッサと、

前記受信機／デコーダの記憶されたＩＤを含むメモリ手段と、

前記記憶されたＩＤと前記スマートカード読み取り器によって読み取られたスマートカードのＩＤとを比較する手段と、

前記比較に応じて前記信号の暗号解読を可能あるいは不可能にする手段とを備えていることを特徴とする受信機／デコーダ。

４１．前記可能化手段が前記スマートカードを使用可能あるいは使用禁止するように構成されている請求項４０に記載の受信機／デコーダ。

４２．前記プロセッサが、前記受信機／デコーダとスマートカード間のハンドシェークルーチンに応じて前記スマートカードを使用可能にするように構成されていることを特徴とする請求項４１に記載の受信機／デコーダ。

４３．前記受信機／デコーダがビデオおよびまたはオーディオ信号を受信し、かつ暗号解読するように構成されている請求項４０～４２のいずれかに記載の受信機／デコーダ。

４４．前記スマートカードが、作動できるそれぞれの受信機／デコーダのＩＤのリストを含むメモリおよび前記スマートカードが前記リストされた受信機／デコーダの各々と作動できるかどうかについての表示を含むことを特徴とする請求項４０～４３のいずれかに記載の受信機／デコーダで使用するためのスマートカード。

４５．前記受信機／デコーダが、前記スマートカードのメモリに列挙された各受信機／デコーダの前記ＩＤを読み取る手段と、前記スマートカードが前記受信機／デコーダと同時に使用できるかどうかを決定するそれに関連した表示とを備えていることを特徴とする請求項４０～４３のいずれかに記載の受信機／デコーダと請求項４４に記載のスマートカードとの組み合わせ。

４６．暗号化放送信号の受信機と併用するためのスマートカードであって、

前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、

前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサが、前記メモリのそれぞれのゾーンの手段によってこのような信号のそれぞれの放送供給者から複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、前記ゾーンの各々が、前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成され、前記暗号解読データが、それぞれの放送供給者によって前記スマートカードに割り当てられた優先順位レベルを含み、かつこの放送供給者によって放送されたこの優先順位レベルに関連した信号の暗号解読を可能にすることを特徴とするスマートカード。

４７．前記優先順位レベルが、前記放送供給者によって放送された制御信号によってスマートカードに割り当てられることを特徴とする請求項４５に記載のスマートカード。

４８．暗号解読放送信号を受信機／デコーダに放送する装置であって、前記受信機／デコーダがそれに割り当てられたそれぞれの優先順位を有するものにおいて、前記装置が、

前記放送信号の暗号解読を制御するかあるいは可能にする制御信号を発生する

手段であって、前記制御信号の各々が、対応するアドレスを有する受信機／デコーダによる暗号解読を選択的に可能にするアドレス部を有することと、

そのそれぞれの優先順位に従って前記制御信号で受信機／デコーダを選択的にアドレス指定する手段とを備えていることを特徴とする暗号解読放送信号を受信機／デコーダに放送する装置。

４９．それぞれの放送供給者の放送信号に関連した第１のセットを構成する制御信号およびそれぞれのプログラムに関連した第２のセットを構成する制御信号を発生する手段をさらに備え、前記第２のセットの制御信号が前記受信機／デコーダによる暗号解読を制御するように構成され、前記第２のセットの制御信号が前記アドレス部を有することを特徴とする請求項４８に記載の装置。

５０．前記装置が選択された地理的な位置における選択プログラムの暗号解読を中止するように構成された請求項４８あるいは４９に記載の装置。

５１．おおむねここで添付図面に関して記載されたスマートカード。

５２．おおむね添付図面の図１および図２に関して前述されたような受信機／デコーダ。

５３．おおむね添付図面の図１および図２に関してここに記載されたような暗号化放送信号を受信機／デコーダに放送する装置。

５４．おおむね添付図面の図１および図２に関してここに記載されたような暗号化放送信号を受信機／デコーダに放送する方法。

【発明の詳細な説明】

暗号化放送信号の受信機と併用するためのスマートカード、および受信機

産業上の利用分野

本発明は、放送・受信システムで暗号化放送信号の受信機と併用するためのスマートカード、放送信号を受信し、暗号化する受信機／デコーダ、暗号化信号を放送する装置および暗号化信号を放送する方法に関するものである。

本発明は、特に他を排斥するものではないが、下記の好ましい特徴のいくつかあるいは全てを有する大量市場放送システムに関するものである。

背景技術

この放送システムは、情報放送システム、好ましくはラジオおよび／またはテレビジョン放送システムである

（この放送システムがケーブル伝送あるいは地上伝送に応用可能し得るけれども）この放送システムは衛星システムである

この放送システムは、好ましくは、データ／信号伝送のためのＭＰＥＧ、より好ましくは、ＭＰＥＧ－２、圧縮システムを使用するディジタルシステムである。

このシステムでは双方向の放送も可能である

この放送システムはスマートカードを使用する

用語“スマートカード”は、ここでは広義で使用され、（そのように排他的ではないが）任意のマイクロプロセッサベースカードあるいは同様な機能および性能のオブジェクトを含んでいる。

発明の開示

第１の態様では、本発明は暗号化放送信号の受信機と併用するためのスマートカードを提供し、スマートカードは、

前記信号を使用可能するかあるいは前記信号の暗号解読を制御するマイクロプロセッサと、

前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサが、前記メモリのそれぞれの動的に作成されたゾーン

によってこのような信号のそれぞれの放送供給者からの複数のこのような個別の暗号解読を可能にするかあるいは制御するように構成され、前記動的に作成されたゾーンの各々は、前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように配置されている。

スマートカードのゾーンの動的作成（および除去）は、例えば、放送局によって周期的に送信され、受信機／デコーダによって受信され、スマートカードに送られるＥＭＭによって容易に、かつ迅速に変えられるスマートカードによって加入者に与えられた権利の為に使用される。

好ましくは、スマートカードは、前記放送供給者のそれぞれの放送供給者に関連した識別子および少なくとも１つの秘密暗号解読キーをさらに備え、前記識別子および前記キーあるいは各キーが、前記動的作成されたゾーンの中の１つに記憶され、この識別子に対応するＩＤを有する放送信号を暗号解読するように構成され、この暗号解読キーに対応する暗号化キーを使用して暗号化される。

スマートカードは、各ゾーンに対して記憶されたグループ識別子と、このグループ内部のグループ識別子を識別し、記憶されたグループ識別子に対応するＩＤを有する放送信号を暗号解読するように構成された他の識別子とをさらに備えている。

スマートカードは、それぞれの放送供給者のＩＤを含むメモリゾーンからなる第１のシリーズおよび動的に作成されたメモリゾーンからなる第２のシリーズを保持するように構成されてもよく、第２のシリーズに於けるメモリゾーンの各々は、放送供給者のＩＤを示すラベルを付けられ、この供給者からの受信放送信号の処理のために使用される前記暗号解読データを含むデータを含み、第２のシリーズにおける複数のメモリゾーンは、共通ＩＤラベルを有し、かつこの放送供給者からの受信放送信号の処理に関する異なる種類のデータを含む。

好ましくは、このスマートカードは、前記第１のシリーズを形成するメモリゾーンを動的に作成するように構成される。この動的に作成されたメモリゾーンは連続的であってもよい。

好ましくは、スマートカードは、前記動的に作成されたゾーンの動的作成を制御するデータを記憶するように構成された管理メモリゾーンを備えている。

前記動的に作成されたゾーンの中の１つはスマートカードのユーザが暗号解読する権利を付与される放送供給者によって放送される特定の放送項目の選択を示す権利データを含んでも良く、且つ、スマートカードは、この供給者によって放送される項目を暗号解読する前記権利データを利用するように構成されている。

トランザクションメモリゾーンは、前記動的に作成されたゾーンに加えてスマートカードに規定されてもよく、このトランザクションメモリは、ユーザの制御の下でスマートカードで生成できるトランザクション出力信号に応じてのみスマートカードのユーザが暗号解読する権利を付与される放送供給者によって放送される項目に関する他の権利データを含んでいる。

スマートカードは、項目が前記トランザクション出力信号の出力に続いて放送される機会の数を計数するカウンタをさらに備え、スマートカードは、前記カウンタによって到達される計数値に応じてこの項目の暗号解読を制御するように構成される。

本発明の第２の態様は、前述のようなスマートカードと併用するための受信機／デコーダを提供し、受信機／デコーダは、スマートカード読み取り機を備え、加入者スマートカードの制御の下で放送暗号化信号を暗号解読するように構成されている。

この受信機／デコーダは、暗号化放送ビデオおよび／またはオーディオ信号を暗号解読し、対応するオーディオおよび／またはオーディオ出力を発生させるように構成されている。

好ましくは、受信機／デコーダは、前記暗号化放送信号を受信する比較的高い帯域幅入力ポートと、出力制御信号を放送送信機に送り返すように構成された比較的低い帯域幅出力ポートとを有する。

好ましくは、受信機／デコーダは、記憶された識別子を含み、対応する記憶された識別子を有するスマートカードとだけ作動するように構成されている。

第３の態様では、本発明は、受信機／デコーダに暗号化信号を放送する装置を提供し、この装置が、２又はそれ以上の種類の放送制御信号を発生する手段を備え、当該制御信号の各種類が、対応するＩＤを有する受信機／デコーダをこのよ

うな種類の制御信号に対して選択的に応答するようにした受信機／デコーダＩＤデータを含み、前記受信機／デコーダＩＤデータの１つあるいはそれ以上のグループの受信／デコーダの全てが、共通の種類の制御信号に応答するように構成されたグループＩＤデータを含み、前記装置には、入力情報に応じて異なるＩＤグループ間に個別の受信機／デコーダを動的に分配するように構成されているデータベース手段が装備されている。

データベース手段は、グループ間の受信機／デコーダの分配を変えるように受信機／デコーダから受信された信号に応答してもよい。

この装置は、前記入力情報に応じてグループ間の受信機／デコーダの分配を変える放送制御信号を放送するように構成されてもよい。

異なる種類の制御信号は放送暗号化データストリームの異なる部分の暗号解読を可能にしてもよい。

好ましくは、入力情報は支払い情報を含んでいる。この種類の制御信号は、異なる放送供給者からの暗号化放送信号を暗号解読するために加入操作を制御する種類を含んでいても良い。

この種類の制御信号は異なる時間フレームの放送暗号化データ信号を暗号解読する購入権を制御する種類も含んでもよい。

好ましくは、暗号化放送信号は、ビデオおよび／またはオーディオ信号であり、この装置は、前記暗号化データ信号を軌道上衛星に送信するように構成されてもよい。

各グループは２５６メンバーまで含んでもよい。

第４の態様では、本発明は、暗号化放送信号を受信する受信機／デコーダを提供し、受信機／デコーダは、グループＩＤを含み、前記グループＩＤに対応するＩＤを有するある種類の放送制御信号に応答し、受信機／デコーダは、他の制御信号に応じてそのグループＩＤを変えるように構成されている。

他の制御信号は放送信号を含み、前記放送信号および前記暗号化放送信号は前記受信機／デコーダによって受信されるように構成されている。

好ましくは、グループＩＤは、受信機／デコーダに取り外しできるように挿入されるスマートカードに記録される。前記暗号化放送信号はビデオおよび／また

はオーディオ信号でもよい。

第５の態様では、本発明は、前述のように受信機／デコーダとともに前述のような装置を含むディジタルデータ信号を放送し、受信するシステムを提供する。

第６の態様では、本発明は、暗号化信号を受信機／デコーダに放送する方法を提供し、この方法は、２つあるいはそれ以上の放送制御信号の種類を発生する工程を含み、当該信号の序番各種類は、対応するＩＤを有する受信機／デコーダを選択的に当該制御信号の種類に応答しうる様にするための、受信機／デコーダＩＤデータを含み、入力情報に応じて異なるＩＤグループ間に個別の受信機／デコーダを動的に分配する。

入力情報は、好ましくは、支払い情報を含み、且つ前記受信機／デコーダをして、暗号化放送ビデオおよび／またはオーディオストリームの一部を選択的に暗号解読せしめうる制御信号を更に含んでいる。

第７の態様では、本発明は、暗号化信号を受信機／デコーダに放送する装置を提供し、この装置は、前記暗号化信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段と、制御信号を前記放送信号内部でそれぞれのプログラム伝送と関連付ける手段とを備え、関連付ける手段は、一連の同じプログラム伝送において各伝送を識別する信号を発生する手段を備えている。

好ましくは、この装置は、暗号解読できる前記一連の伝送数に対する制限を受信機／デコーダに設定する信号を発生する手段をさらに備えている。この装置は、前記制限を変えるように受信機／デコーダからの入力信号に応答してもよい。

好ましくは、この装置は、前記ビデオおよび／またはオーディオストリームを軌道上衛星に送信するように構成されている。

第８の態様において、本発明は、放送信号をペイ・パー・ビュー（ＰＰＶ）モードで受信し、かつ暗号解読する受信機／デコーダを提供し、当該受信機／デコーダは、前記放送信号内部で特定のプログラム伝送の暗号解読を可能にするかあるいは制御する制御信号を検出する手段を含み、前記制御信号が一連の同一プログラムの伝送における各伝送を識別する情報を含むことと、前記検出手段に結合され、暗号解読されうる前記一連の伝送数を制限する制限手段とを備えている。

好ましくは、制限手段は、前記シリーズ内の伝送の各連続視聴に応じて記憶された制限値に向けて増減されるように構成されるカウンタを備えている。

又、当該制限手段は、受信放送信号に応じて前記制限値を調整する手段をさらに備えている。

好ましくは、制限手段は、前記一連内部の伝送の各連続視聴に応じて記憶された制限値の方へ増減されるように構成されたカウンタを備えている。受信機／デコーダは、好ましくは、受信放送信号に応じて前記制限値を調整する手段を備えている。

好ましくは、制限手段は、受信機／デコーダに取り外しできるように挿入されたスマートカードを備えている。

第９の態様において、本発明は、暗号化放送信号を受信し、暗号解読する受信機／デコーダを提供し、この受信機／デコーダは、

スマートカードと、

スマートカードに結合され、かつスマートカードからの出力に応じて前記信号を暗号解読するように構成されているプロセッサと、

受信機／デコーダの記憶ＩＤを含むメモリ手段と、

前記記憶臆されたＩＤとスマートカード読み取り器によって読み取られたスマートカードのＩＤとを比較する手段と、

比較に応じて前記信号の暗号解読を可能にするかあるいは不可能にする手段とを備えている。

可能化手段は前記スマートカードを使用可能あるいは使用禁止にするように構成されてもよい。

プロセッサは、受信機／デコーダとスマートカードとの間のハンドシェークに応じて前記スマートカードを使用可能にするように構成されてもよい。

受信機／デコーダは、放送ビデオおよび／またはオーディオ信号を受信し、暗号解読するように構成されてもよい。

第１０の態様において、本発明は、前述のように受信機／デコーダで使用するためのスマートカードを提供し、前記スマートカードは、スマートカードが操作

できるそれぞれの受信機／デコーダのＩＤのリストを含むメモリと、スマートカードが前記リストされた受信機／デコーダの各々で操作できるかどうかに関する表示とを含む。

第１１の態様において、本発明は、前述のような受信機／デコーダと前述のようなスマートカードとの組み合わせを提供し、前記受信機／デコーダは、前記スマートカードのメモリにリストされた各受信機／デコーダのＩＤを読み取る手段と、スマートカードが受信機／デコーダと併用されてもよいかどうかを決定するそれに関連した表示とをさらに備えている。

第１２の態様において、本発明は、暗号化放送信号の受信機と併用するためのスマートカードを提供し、このスマートカードは、

前記信号の暗号解読を可能にするかあるいは制御するマイクロプロセッサと、

前記マイクロプロセッサに結合されたメモリとを備え、

前記マイクロプロセッサは、前記メモリのそれぞれのゾーンによってこのような信号のそれぞれの放送供給者からの複数のこのような信号の個別の暗号解読を可能にするかあるいは制御するように構成され、前記ゾーンの各々が前記放送供給者の中のそれぞれの放送供給者に関連した暗号解読データを記憶するように構成され、前記暗号解読データは、それぞれの放送供給者によってスマートカードに割り当てられた優先順位レベルを含み、この放送供給者によって放送された優先順位レベルに関連した信号の暗号解読を可能にする。

この優先順位のレベルは、放送供給者によって放送された制御信号によってスマートカードに割り当てられてもよい。

第１３の態様において、本発明は、暗号化放送信号を受信機／デコーダに放送する装置を提供し、前記受信機／デコーダはそれに割り当てられたそれぞれの優先順位を有し、この装置は、

前記放送信号の暗号解読を制御するかあるいは可能にする制御信号を発生する手段であって、前記制御信号の各々は対応するアドレスを有する受信機／デコーダによって暗号解読を選択的に可能にするアドレス部を有することと、

そのそれぞれの優先順位レベルに従って前記制御信号で受信機／デコーダを選

択的にアドレス指定する手段とを備えている。

この装置は、放送信号のそれぞれの放送供給者に関連した第１のセットを構成する制御信号およびそれぞれに関連した第２のセットを構成する制御信号を発生する手段をさらに備えてもよく、第２のセットにおける制御信号が受信機／デコーダによる暗号解読をゲートで制御するように構成されたスイッチング部を有し、前記第２のセットの制御信号は前記アドレス部を有する。

この装置は選択された地理的な位置で選択されたプログラムの暗号解読を停止するように構成されてもよい。

図面の簡単な説明

図１は、本発明の好ましい実施例によるディジタルテレビジョンシステムの全アーキテクチャを示している。

図２は、ディジタルテレビジョンシステムの条件付アクセスシステムのアーキテクチャを示している。

図３は、条件付アクセスシステムで使用された権利付与管理メッセージの構造を示している。

図４は、本発明の好ましい実施例による加入者許可システム（ＳＡＳ）のハードウェアの概略図である。

図５は、ＳＡＳのアーキテクチャの概略図である。

図６は、ＳＡＳの一部を形成する加入者技術管理サーバの概略図である。

図７は、ＳＡＳによって実行されるような加入の自動更新のための手順の流れ図である。

図８は、自動更新手順で使用されたグループ加入ビットマップの概略図である。

図９は、自動更新手順で使用されたＥＭＭの構造を示している。

図１０は、ＥＭＭの構造を詳細に示している。

図１１は、通信サーバを通して直接コマンドを受信するために使用される場合の注文集中化サーバの概略図である。

図１２は、本発明の一実施例を示す図２の一部を概略的に示している。

図１３は、コールバックをリクエストするように加入者許可システムからのコ

マンドを受信するために使用される場合の注文集中化サーバの概略図である。

図１４は、通信サーバの概略図である。

図１５は、ＥＭＭ放出サイクル速度がＰＰＶイベントのタイミングにより変更される方法を示している。

図１６は、ＥＭＭを放出するために使用されるメッセージ放出器の概略図である。

図１７は、メッセージ放出器内部のＥＭＭの記憶の方法を示す概略図である。

図１８は、スマートカードの概略図である。

図１９は、スマートカードのメモリゾーンの配置の概略図である。

図２０は、ＰＰＶイベント説明の概略図である。

発明を実施する為の最良の態様

本発明の好ましい特徴は、次に単に例として添付図面を参照して述べられる。

本発明によるディジタルテレビジョン放送・受信システム１０００の概略が図１に示されている。本発明は、圧縮ディジタル信号を送信するために既知のＭＰＥＧ－２を使用する主に従来のディジタルテレビジョンシステム２０００を含んでいる。より詳細には、放送センターのＭＰＥＧ－２圧縮器２００２は、ディジタル信号ストリーム（一般的にはビデオ信号のストリーム）を受信する。この圧縮器２００２は、リンケージ２００６によってマルチプレクサ・スクランブラ２００４に接続されている。マルチプレクサ２００４は、複数の他の入力信号を受信し、１つあるいはそれ以上のトランスポートストリームを組み立て、テレコムリンクを含む様々な形式をとることができるリンケージ２０１０を介して放送センターの送信機２００８に圧縮ディジタル信号を送信する。送信機２００８は、電磁信号が電子的に処理され、従来はエンドユーザによって所有されるかあるいは賃貸された皿形の地上受信機２０１８に概念的なダウンリンク２０１６を介して放送する。受信機２０１８によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸された複合受信機／デコーダ２０２０に送信され、エンドユーザのテレビジョンセット２０２２に接続されている。この受信機／デコーダ２０２０は、圧縮ＭＰＥＧ－２信号をテレビジョンセット２０２２のための

テレビジョン信号に復号化する。

条件付アクセスシステム３０００は、マルチプレクサ２００４および受信機／デコーダ２０２０に接続され、一部は放送センターに、一部はデコーダに置かれている。条件付アクセスシステム３０００は、エンドユーザが１つあるいはそれ以上の放送供給者からのディジタルテレビジョン放送にアクセスすることを可能にする。商業オファー（すなわち、放送供給者によって販売された１つあるいはいくつかのテレビジョンプログラム）に関するメッセージを解読できるスマートカードは受信機／デコーダ２０２０に挿入できる。デコーダ２０２０およびスマートカードを使用して、エンドユーザは、加入モードあるいはペイ・パー・ビューモードのいずれかのイベントを購入できる。

マルチプレクサ２００４および受信機／デコーダ２０２０にも接続され、さらに一部は放送センターに置かれ、一部はデコーダに置かれている対話式システム４０００によって、エンドユーザはモデムバックチャネル４００２を介して様々なアプリケーションと対話できる。

条件付アクセスシステム３０００は、次により詳細に述べられる。

図２を参照するに、概略において、条件付アクセスシステム３０００は、加入者許可システム（ＳＡＳ）３００２を含んでいる。ＳＡＳ３００２は、それぞれのＴＣＰ－ＩＰリンケージ３００６（その代わりに他のリンケージのタイプが使用できるけれども）によって１つあるいはそれ以上の加入者管理システム（ＳＭＳ）３００４に接続される。１つのＳＭＳは各々の放送供給者に対するものである。その代わりに、１つのＳＭＳは２つの放送供給者間に共有することができるか、あるいは１つの供給者は２つのＳＭＳ等を使用できる。

「マザー」スマートカードを利用する暗号化装置３００８の形の第１の暗号化装置は、リンケージ３０１２によってＳＡＳに接続されている。また、マザースマートカード３０１６を利用する暗号化装置３０１４の形の第２の暗号化装置はリンケージ３０１８によってマルチプレクサ２００４に接続されている。受信機／デコーダ２０２０は「ドーター」スマートカード３０２０を受け取る。受信機／デコーダ２０２０は、モデムバックチャネル４００２を介して通信サーバ３０

２２によってＳＡＳ３００２に直接接続される。ＳＡＳは、要求に応じてドータースマートカードに加入権を送信する。

このスマートカードは１つあるいはそれ以上の商業オペレータの秘密を含む。

「マザー」スマートカードは異なる種類のメッセージを暗号化し、「ドーター」スマートカードは、このスマートカードがメッセージを解読する権利を有するならば、メッセージを解読する。

第１および第２の暗号化装置３００８および３０１４は、ラックと、ＥＥＰＲＯＭ上に記憶されたソフトウェアを有するＶＭＥカードと、２０枚までの電子カードおよび各電子カードに対してそれぞれＥＣＭを暗号化するカード（カード３０１６）と、ＥＭＭを暗号化するカード（カード３０１０）の１枚のスマートカード３０１０および３０１６とを含む。

ディジタルテレビジョンシステムの条件付アクセスシステム３０００の動作は、次にテレビジョンシステム２０００および条件付アクセスシステム３０００の様々な構成要素を参照してより詳細に述べられる。

マルチプレクサ・スクランブラ

図１および図２に参照すると、放送センターにおいて、ディジタルビデオ信号は、ＭＰＥＧ－２圧縮器２００２を使用して、最初に圧縮される（あるいはビットレート減少される）。この圧縮信号は、次に他の圧縮データのような他のデータで多重化されるためにリンケージ２００６を介してマルチプレクサ・スクランブラ２００４に伝送される。

このスクランブラは、スクランブル処理で使用され、マルチプレクサ２００４においてＭＰＥＧ－２ストリームに含まれた制御語を生成する。この制御語は、内部で生成され、ユーザの統合受信機／デコーダ２０２０がプログラムを暗号解読することを可能にする。

いかにプログラムが商品化されるかを示すアクセス基準はＭＰＥＧ－２ストリームにも付加される。このプログラムは、多数の「加入」モードの中の１つおよび／または多数の「ペイ・パー・ビュー」（ＰＰＶ）モードあるいはイベントの中の１つのいずれかで商品化されてもよい。

加入モードでは、エンドユーザは、１つあるいはそれ以上の商業オファー、すなわち「ブーケ」（ｂｏｕｑｕｅｔ）を申し込むので、これらのブーケ内部のあらゆるチャネルを見る権利を得る。

好ましい実施例では、９６０までの商業オファーはチャネルのブーケから選択されてもよい。ペイ・ビュー・ビューモードでは、エンドユーザには、望むようなイベントを購入する機能が提供される。これは、イベントを前もってプレブックすることあるいはイベントが放送されるや否や購入することのいずれかによって行うことができる。好ましい実施例では、全てのユーザが加入モードあるいはＰＰＶモードで見ても見なくても、全てのユーザは加入者であるが、もちろん、ＰＰＶ視聴者は必ずしも加入者である必要がない。

制御語およびアクセス基準の両方は、権利付与制御メッセージ（ＥＣＭ）を形成するために使用される。すなわちこれは１つのスクランブルプログラムとの関連で送信されるメッセージである。すなわちこのメッセージは、放送プログラムの（プログラムのデスクランブルを可能にする）制御語およびアクセス基準を含む。アクセス基準および制御語は、リンケージ３０１８を介して第２の暗号化装置３０１４に伝送される。この装置では、ＥＣＭは生成され、暗号化され、マルチプレクサ・スクランブラ２００４上に伝送される。

データストリームにおける放送供給者によって放送される各サービスは多数の別個の構成要素を含んでいる。すなわち、例えば、テレビジョンプログラムは、ビデオ構成要素、オーディオ構成要素、サブタイトル構成要素等を含んでいる。サービスのこれらの構成要素の各々は、トランスポンダ２０１４にその後に放送するために個別にスクランブルされ、暗号化される。サービスの各スクランブルされた構成要素に関しては、別個のＥＣＭが要求される。

プログラム送信

マルチプレクサ２００４は、ＳＡＳ３００２からの暗号化ＥＭＭと、第２の暗号化装置３０１４からの暗号化ＥＣＭと圧縮器２００２からの圧縮プログラムとを含む電気信号を受信する。マルチプレクサ２００４は、プログラムをスクランブルし、スクランブルされたプログラム、暗号化ＥＭＭおよび暗号化ＥＣＭを電

気信号として放送センターの送信機２００８にリンケージ２０１０を介して送信する。送信機２００８は、アップリンク２０１２を介して衛星トランスポンダ２０１４の方へ電磁信号を送信する。

プログラム受信

衛星トランスポンダ２０１４は、送信機２００８によって送信された電磁信号を受信し、処理し、ダウンリンク２０１６を介して、従来はエンドユーザによって所有されるかあるいは賃貸された皿形の地上受信機２０１８上に送信する。受信機２０１８によって受信された信号は、エンドユーザによって所有されるかあるいは賃貸された統合受信機／デコーダ２０２０に送信され、エンドユーザのテレビジョンセット２０２２に接続される。この受信機／デコーダ２０２０は、暗号化ＥＭＭおよび暗号化ＥＣＭを有するスクランブルされたプログラムを得るために信号を多重分離する。

プログラムがスクランブルされない場合、すなわち、ＥＣＭがＭＰＥＧ－２ストリームとともに全く送信されない場合、受信機／デコーダ２０２０は、データを分解し、この信号をテレビジョンセット２０２２に送信するためのビデオ信号に変換する。

プログラムがスクランブルされる場合、受信機／デコーダ２０２０は、対応するＥＣＭをＭＰＥＧ－２ストリームから抽出し、ＥＣＭをエンドユーサの「ドーター」スマートカード３０２０に送る。これは、受信機／デコーダ２０２０のハウジングにうまくはまる。ドータースマートカード３０２０は、エンドユーザがＥＣＭを暗号解読し、プログラムにアクセスする権利を有するかどうかを制御する。有していない場合、負の状態は、受信機／デコーダ２０２０に送られ、プログラムが暗号解読できないことを示す。エンドユーザが権利を有する場合、ＥＣＭは暗号解読され、制御語が抽出される。次に、デコーダ２０２０は、この制御語を使用してプログラムを暗号解読できる。ＭＰＥＧ－２ストリームは、伸長され、テレビジョンセット２０２２に前方送信するためのビデオ信号に変換される。

加入者管理システム（ＳＭＳ）

加入者管理システム（ＳＭＳ）３００４は、特にエンドユーザファイル、商業オファー（例えば、料金およびプロモーション）、加入、ＰＰＶ詳細、エンドユーザ消費および許可に関するデータの全てを管理するデータベース３０２４を含んでいる。ＳＭＳは、物理的にＳＡＳから遠隔であってもよい。

各ＳＭＳ３００４は、エンドユーザに送信される権利付与管理メッセージ（ＥＭＭ）の変更あるいは形成を意味するメッセージをそれぞれのリンケージ３００６を介してＳＡＳ３００２に送信する。

ＳＭＳ３００４は、ＥＭＭの変更およびＥＭＭの形成を意味せず、（製品を注文する場合、エンドユーザに付与された許可あるいはエンドユーザが請求される額に関する）エンドユーザの状態の変化のみを意味するメッセージをＳＡＳ３００２にも送信する。

後述されるように、ＳＡＳ３００２は、（一般的にはコールバック情報あるいは課金情報のような情報を要求する）メッセージをＳＭＳ３００４に送信するので、２つの間の通信が双方向であることは明らかである。

エンタイトルメントマネージメントメッセージ（ＥＭＭ）

ＥＭＭは、（１つのスクランブルされたプログラムだけ、あるいは同じ商業オファーの一部である場合にはスクランブルされたプログラムのセットに専用であるＥＣＭと対比して）個人エンドユーザ（加入者）、あるいはエンドユーザのグループに専用のメッセージである。各グループには所定数のエンドユーザが含まれる。

グループとしてのこの構成はバンド幅を最適化することを目指している。

すなわち、１つのグループへのアクセスは多数のエンドユーザへの到達を可能にできる。

様々な特定のタイプのＥＭＭは、本発明を実施する際に使用される。個人ＥＭＭは個人加入者に専用であり、一般的にはペイ・パー・ビューサービスと共に使用される。

すなわち、これらは、このグループのグループ識別子および加入者の位置を含む。いわゆる「グループ」加入ＥＭＭは、例えば、２５６人の個人ユーザのグル

ープに専用であり、一般的にはいくつかの加入サービスの管理に使用される。

ＥＭＭは、グループ識別子および加入者のグループビットマップを有する。聴衆ＥＭＭは、全聴衆に専用であり、例えば、ある種の無料サービスを提供するために特定のオペレータによって使用されてもよい。

「聴衆」は、同じオペレータ識別子（ＯＰＩ）を搭載するスマートカードを有する全体の加入者である。最後に、「ユニーク」ＥＭＭはスマートカードのユニーク識別子に向けられる。典型的なＥＭＭの構造は、次に図３を参照して述べられる。基本的には、一連のディジタルデータビットとして実現されるＥＭＭは、

ヘッダ３０６０と、ユニークＥＭＭ３０６２と、シグネチャ３０６４とを含む。次に、ヘッダ３０６０は、タイプが個人、グループ、聴衆あるいは若干の他のタイプであるかどうかを識別するタイプ識別子３０６６と、ＥＭＭの長さを示す長さ識別子３０６８と、ＥＭＭのための任意のアドレス３０７０と、オペレータ識別子３０７２と、キー識別子３０７４とを含む。ユニークＥＭＭ３０６２は、もちろんそのタイプに従って大いに変わる。最後に、一般的には８バイトの長さであるシグネチャ３０６４は、ＥＭＭの残りのデータの破損に対して多数のチェックを行う。

加入者許可システム（ＳＡＳ）

ＳＭＳ３００４によって生成されたメッセージは、リンケージ３００６を介して加入者許可システム（ＳＡＳ）３００２に送られ、この加入者許可システム（ＳＡＳ）３００２は、次にＳＭＳ３００４によって生成されたメッセージの受信を肯定応答するメッセージを生成し、これらの肯定応答をＳＭＳ３００４に送る。

図４に示されるように、ハードウェアレベルで、ＳＡＳは、既知の方法で、データおよびコマンド入力のための１つあるいはそれ以上のキーボード３０５２に接続されたメインフレームコンピュータ３０５０（好ましい実施例では、ＤＥＣマシン）と、出力情報の表示のための１つあるいはそれ以上の表示装置（ＶＤＵ）３０５４と、データ記憶手段３０５６とを備えている。ハードウェアにある程度の冗長性が与えられてもよい。

ソフトウェアレベルで、ＳＡＳは、好ましい実施例では、標準オープンＶＭＳオペレーティングシステム、すなわちそのアーキテクチャが次に図５を参照して概説で述べられる一連のソフトウェアで実行する。すなわち、ソフトウェアがその代わりにハードウェアで実現できることが理解される。

概説において、ＳＡＳは、加入モードのための権利を与え、毎月この権利を自動的に更新する加入チェーン領域３１００と、ＰＰＶイベントのための権利を与えるペイ・パー・ビューチェーン領域３２００と、加入・ＰＰＶチェーン領域によって形成されたＥＭＭをマルチプレクサ・スクランブラ２００４に送るので、ＥＭＭを有するＭＰＥＧストリームを供給するＥＭＭインジェクタ３３００とを備えている。

ユーザのパーソナルコンピュータにコンピュータソフトウェアをダウンロードする場合のペイ・パー・ファイル（ＰＰＦ）権利のような他の権利が付与されるべきである場合、他の同様な領域も装備される。

ＳＡＳ３００２の１つの機能は、加入モードで商業オファーとして利用されるかあるいは異なる商品化のモード（プレブックモード、インパルスモード）によるＰＰＶイベントとして販売されるテレビジョンプログラムへのアクセス権を管理することにある。これらの権利およびＳＭＳ３００４から受信された情報により、ＳＡＳ３００２は、加入者のためのＥＭＭを生成する。

加入チェーン領域３１００は、コマンドインタフェース（ＣＩ）３１０２と、加入者技術管理（ＳＴＭ）サーバ３１０４と、メッセージ生成器（ＭＧ）３１０６と、暗号化装置３００８とを備えている。ＰＰＶチェーン領域３２００は、許可サーバ（ＡＳ）３２０２と、エンドユーザの関連詳細を記憶するリレーショナルデータベース３２０４と、データベースのためのローカルブラックリストデータベース３２０５と、データベースのためのデータベースサーバ３２０６と、注文集中化サーバ（ＯＣＳ）３２０７と、プログラム放送器のためのサーバ（ＳＰＢ）３２０８と、その機能が加入チェーン領域のための機能と基本的に同じであるので、さらに少しも詳述されないメッセージ生成器（ＭＧ）３２１０と、暗号化装置３００８とを備えている。

ＥＭＭインジェクタ３３００は、複数のメッセージ放出器３３０２、３３０４、３３０６および３３０８およびソフトウェアマルチプレクサ（ＳＭＵＸ）３３１０および３３１２を備えている。好ましい実施例では、メッセージ生成器３２１０のための他の２つのＭＥ３３０６および３３０８とともにメッセージ生成器３１０６のための２つのＭＥ３３０２および３３０４がある。ＭＥ３３０２および３３０６は、ＳＭＵＸ３３１０に接続されるのに対して、ＭＥ３３０４および３３０８はＳＭＵＸ３３１２に接続される。

ＳＡＳの３つの主要構成要素（加入チェーン領域、ＰＰＶチェーン領域およびＥＭＭインジェクタ）の各々は、次により詳細に考察される。

加入チェーン領域

最初に加入チェーン領域３１００を考察すると、コマンドインタフェース３１０２は、主にＳＭＳ３００４からＳＴＭサーバ３１０４ならびにＯＣＳ３２０６に、およびＯＣＳからＳＭＳにメッセージを急送するためのものである。コマンドインタフェースは、ＳＭＳからの入力として直接コマンドあるいはコマンドを含むバッチファイルをとる。コマンドインタフェースは、ＳＴＭサーバからくるメッセージで構文分析を実行し、エラーがメッセージで生じる場合、正確なメッセージを放出できる（範囲外のパラメータ、見つからないパラメータ等）。コマンドインタフェースは、一連のコマンドを再生できるようにトレースファイル３１１０におけるテキスト形式の入力コマンドおよび再生ファイル３１１２における２進形式の入力コマンドもトレースする。トレースは使用禁止され、ファイルのサイズは制限される。

ＳＴＭサーバ３１０４の詳細は、次に特に図６を参照して述べられる。効果的にはＳＴＭサーバは加入チェーン領域の主エンジンであり、無料権利を管理する目的、新規の加入者の作成、および現在の加入者の更新を有する。

図で示されるように、コマンドは、コマンドがＳＴＭサーバに送られるフォーマットとは異なるフォーマットであるが、メッセージ生成器３１０６に渡される。

各コマンドに関しては、ＳＴＭサーバは、関連コマンドが効果的に処理され、

ＭＧに送られる場合だけ肯定応答メッセージをＣＩに送信するように構成されている。

ＳＴＭは、加入者の全ての関連パラメータ（スマートカード番号、商業オファー、状態、グループおよびグループの位置等）が記憶される加入者データベース３１２０を含む。このデータベースは、データベースの内容に対してＣＩ３１０２によって送信されたコマンドの意味チェックを実行し、コマンドが有効である場合、データベースを更新する。

ＳＴＭサーバは、ＳＴＭサーバとＭＧとの間のファーストインファーストアウト（ＦＩＦＯ）バッファ３１２２ならびにバックアップディスクＦＩＦＯ３１２４をさらに管理する。ＦＩＦＯの目的は、ＭＧが任意の理由のためにしばらく応答できない場合、ＣＩからのコマンドの流れを平均化することにある。ＦＩＦＯは、再開始される場合、ＳＴＭサーバはそのＦＩＦＯを空にする（すなわち、ＭＧに送信する）ように構成されているので、ＳＴＭサーバあるいはＭＧがクラッシュした場合、コマンドが全く失われないことも確実にすることができる。ＦＩＦＯはファイルとして実現される。

ＳＴＭサーバは、更新およびオペレータによって要求されるならば、無料権利を自動的に生成する自動更新サーバ３１２６をその中心部に含む。これに関連して、新規の権利の生成がＳＭＳで開始されることが理解されるけれども、更新の生成は、初めて権利の生成を含むものとみなすことができる。明らかになるように、２つはおよそ同じコマンドおよびＥＭＭによって処理できる。

重要な機能は、ＳＭＳからＳＡＳに送られることが必要であるコマンドの数を著しく減らすことができるので（ＳＭＳおよびＳＡＳが異なる位置にあり、異なるオペレータによって操作されてもよいことを覚えておく）、ＳＡＳから離れたＳＴＭおよびＳＭＳ３００４において（既知システムにおいて）よりもむしろＳＡＳ内部の自動更新サーバを有することは特に重要な機能である。

実際、ＳＭＳから要求された２つの主コマンドは、新規の加入が開始されるべきであり、現在の加入が停止されるべき（例えば、未払いの場合）である単なるコマンドである。ＳＭＳとＳＡＳとの間のコマンド交換を最少にすることによっ

て、２つの間のリンケージ３００６におけるコマンド転送の障害の可能性が減少される。さらに、ＳＭＳの設計は、条件付アクセスシステム３０００の機能を一般に考慮する必要がない。

自動更新は図７の流れ図に示されたように進行する。バンド幅を減らすために、全更新の中の非常に高いパーセンテージが標準である場合、更新は加入者のグループにおいて進行する。

すなわち、好ましい実施例では、グループ毎に２５６人の個人加入者がある。流れ図は、開始ステップ３１３０で開始し、毎月の更新機能の作動が行われるステップ３１３２に進む（もちろん、他の回数でも可能であることが理解されるけれども）。毎月の頻度で、権利は、エンドユーザに現在の月および次の月の全ての間に与えられ、その時点で権利が、更新されない場合は、終了する。

ステップ３１３４で、加入者データベース３１２０は、特定の個人のための権利が更新されるべきであるかどうかを決定するために各グループおよびこのグループ内部の各個人に関してアクセスされる。

ステップ３１３６で、グループ加入ビットマップは、図８に示されるように加入者データベースの内容により設定される。このビットマップは、グループ識別子（この場合、グループ１－「Ｇ１」）３１３８および２５６の個人加入者ゾーン３１４０を含んでいる。ビットマップの個別のビットは、特定の加入者が更新される権利を有するべきであるか否かにより１あるいは０にセットされる。典型的な２進データのセットはこの図に示されている。

ステップ３１４２で、グループ加入ビットマップを含む適当なコマンドは、メッセージ生成器３１０６に送られる。ステップ３１４３で、メッセージ生成器は、特定の加入ＥＭＭが有効でない日付をスマートカードを表示するように陳腐化日付を設定する。すなわち、一般的には、この日付は、次の月の末日として設定される。

ステップ３１４４で、メッセージ生成器は、コマンドから適当なグループ加入ＥＭＭを発生し、暗号化装置３００８にＥＭＭを暗号化するように求め、それから、暗号化ＥＭＭは、ステップ３１４６で、ＥＭＭをＭＰＥＧ－２データストリ

ームに入れるＥＭＭインジェクタ３３００に送られる。

ステップ３１４８は、前述の手順が各グループおよび毎グループに対して繰り返されることを示している。

実際、図７を参照して前述された流れ図は、特に加入の更新に関するものである。ＳＴＭも同様に無料聴衆権利および新規加入者を管理する。

特定のテレビジョンプログラムあるいはこのようなプログラムのグループに役に立つ無料聴衆権利の場合、これらは、コマンドをメッセージ生成器に出し、所与の日数（あるいは週数）の陳腐化日付を有する適当な聴衆ＥＭＭ（全聴衆に対して）を発生するＳＴＭによって利用される。ＭＧは、ＳＴＭコマンドに基づいて正確な陳腐化日付を計算する。

新規加入者の場合、これらは２つの工程で処理される。まず第一に、買物の際に、受信機／デコーダ２０２０におけるスマートカード（所望ならば、オペレータによって）は、所与の期間（一般的には２、３日）加入者無料権を与える。これは、関連陳腐化日付を含む加入者のためのビットマップを生成することによって実行される。

次に、加入者は、完了された事務手続きを、加入者を（ＳＭＳで）管理するオペレータに渡す。一旦事務手続きが処理されると、ＳＭＳは、この特定の加入者のための開始コマンドをＳＡＳに供給する。開始コマンドのＳＡＳによる受信の際、ＳＴＭは、ＭＧに命令し、ユニークアドレスを新規加入者（特定のグループ番号およびグループ内部の位置を有する）に割り当て、（更新のために使用されたより普通の「グループ」加入ＥＭＭとは対照的に）特別のいわゆる「商業オファー」加入ＥＭＭを生成し、次の月の月末まで、特定の加入者に権利を与える。

この時点から、加入者の更新は前述のように自動的に生じ得る。この２つの工程処理によって、ＳＭＳが停止コマンドを発するまで、新規加入者権利を付与することができる。

商業オファー加入ＥＭＭが新規加入者および現在の加入者の再アクティベーションのために使用されることに注目すべきである。グループ加入ＥＭＭは更新目的および停止目的のために使用される。

図９を参照すると、前述の手順によって生成された典型的なユニーク加入ＥＭＭ（すなわち、ヘッダおよびシグネチャを無視する）は、下記の主要な部分、すなわち、一般的には２５６ビットの加入（あるいは加入者のグループ）ビットマップ３１５２と、ＥＭＭの暗号化のための１２８ビットの管理暗号化キー３１５４と、放送プログラムにアクセスするためにスマートカード３０２０が制御語を暗号解読できる６４ビットの各利用暗号化キー３１５６と、スマートカードがＥＭＭを無視する日付を表示する１６ビットの陳腐化日付３１５８とを含んでいる。

実際、好ましい実施例では、３つの利用キーが備えられ、１つのキーが今月のためにセットされ、１つのキーが来月のためにセットされ、１つのキーがシステム障害の場合の再開目的のためのものである。

より詳細には、グループ加入ユニークＥＭＭは、管理暗号化キー３１５４を除いて上記の構成要素の全てを有する。商業オファー加入ユニークＥＭＭ（個人加入者のためのものである）は、全加入者のグループビットマップ３１５２の代わりにグループにおける位置が続くグループＩＤを含み、それから関連陳腐化日付３１５８が続く管理暗号化キー３１５４および３つの利用キー３１５６を含んでいる。

メッセージ生成器３１０６は、ＳＴＭサーバによって発されたコマンドをメッセージ放出器３３０２に送るためのＥＭＭに変換するのに役立つ。図５を参照すると、まず第一に、ＭＧは、ユニークＥＭＭを発生し、これを管理キーおよび利用キーに関して暗号化する暗号化装置３００８に送る。ＣＵは、ＥＭＭのシグネチャ３０６４（図３を参照）を完了し、ＥＭＭをヘッダ３０６０が付加されるＭＧに返送する。したがって、メッセージ放出器に送られたＥＭＭは全ＥＭＭである。メッセージ生成器も、放送開始・中止時間およびＥＭＭの放出速度を決定し、これらをＥＭＭとともに適当な指令としてメッセージ放出器に送る。ＭＧだけが所与のＥＭＭを１回発生する。すなわち、それは周期的送信を実行するＭＥである。

再度、図５を参照すると、メッセージ生成器は、関連ＥＭＭの存続期間、それ

を記憶するそれ自体のＥＭＭデータベース３１６０を含む。一旦その放出持続期間が満了すると、関連ＥＭＭが削除される。データベースは、ＭＧとＭＥとの間の整合性を確実にするために使用されるので、例えば、エンドユーザが資格を一時的に取り上げられる場合、ＭＥは更新を送信し続けない。この点では、ＭＧは関連演算を計算し、これをＭＥに送信する。

ＥＭＭの生成の際に、ＭＧはユニーク識別子をＥＭＭに割り当てる。ＭＧはＥＭＭをＭＥに送る場合、ＭＧもＥＭＭ　ＩＤを送る。これは、ＭＧおよびＭＥの両方で特定のＥＭＭの識別を可能にする。

さらに、加入チェーン領域に関しては、メッセージ生成器は、暗号化ＥＭＭを記憶する２つのＦＩＦＯ３１６２および３１６４を含み、このＦＩＦＯはＥＭＭインジェクタ３３００における関連メッセージ放出器３３０２および３３０４の各々のためのものである。加入チェーン領域およびＥＭＭインジェクタは、かなりの距離を隔てて離れてもよいので、たとえ２つの間のリンク３１６６および３１６８が故障するとしても、ＦＩＦＯの使用はＥＭＭ送信において完全な連続性を可能にすることができる。同様なＦＩＦＯはペイ・パー・ビューチェーン領域に備えられる。

特にメッセージ発生器および一般に条件付アクセスシステムの１つの特定の機能は、空間を節約するパラメータ長および識別子を混合することによってユニークＥＭＭ３０６２の長さを減少する方法に関するものである。これは、次に、典型的なＥＭＭ（実際、最も簡単なＥＭＭであるＰＰＶ　ＥＭＭ）を示す図１０を参照して述べられる。長さの減少は、Ｐｉｄ（パケットあるいは「パラメータ」識別子）３１７０て生じる。

これは、２つの部分、すなわち実際のＩＤ３１７２およびパケットのための長さパラメータ３１７４（次のパケットの開始が識別することができるために必要である）を含む。全Ｐｉｄは、ちょうど１バイトの情報で示される。すなわち、４ビットはＩＤのために用意され、４ビットが長さのために用意される。４ビットは真の２進法で長さを規定するには十分でないので、ビットと実際の長さとの間の異なる相応関係が使用され、この相応関係は、メッセージ生成器における記

憶領域３１７８に記憶されたルックアップテーブルに示されている（図５を参照）。相応関係は、一般的には下記の通りである。

００００＝０

０００１＝１

００１０＝２

００１１＝３

０１００＝４

０１０１＝５

０１１０＝６

０１１１＝７

１０００＝８

１００１＝９

１０１０＝１０

１０１１＝１１

１１００＝１２

１１０１＝１６

１１１０＝２４

１１１１＝３２

長さパラメータはパケットの実際の長さに正比例していないことが分かる。この関係は部分的には線形よりもむしろより方形のようである。これにより、より大きな範囲のパケットの長さが提供される。

ペイ・パー・ビューチェーン領域

ペイ・パー・ビューチェーン領域３２００に関しては、図５をより詳細に参照すると、許可サーバ３２０２は、ＰＰＶ製品を購入するために通信サーバ３０２２に接続する各加入者についての情報を要求する注文集中化サーバ３２０７をそのクライアントとして有する。

加入者がＡＳ３２０２から識別されるならば、トランザクションのセットが行われる。加入者が注文を許可された場合、ＡＳは請求書を作成し、それをＯＣＳ

に送る。さもなければ、ＡＳは注文が許可されないという信号をＯＣＳに送出する。

少なくとも１つのトランザクションが許可された場合、ＡＳがデータベースサーバ（ＤＢＡＳ）３２０６を介してエンドユーザデータベース３２０４を更新することは、このトランザクションのセットの終了時だけである。これにより、データベースアクセス数が最適化される。

ＡＳが購入を許可する基準は、ＤＢＡＳ処理を通してアクセスされるデータベースに記憶される。１つの実施例では、データベースはＳＴＭによってアクセスされるデータベースと同じである。

消費者プロフィールに応じて、許可は否定されてもよい(ＰＰＶ＿Ｆｏｒｂｄｄｅｎ，Ｃａｓｉｎｏ＿Ｆｏｒｂｉｄｄｅｎ．．．)。これらの種類の基準は、ＳＭＳ３００４のためにＳＴＭ３１０４によって更新される。

購入のために許可された限界などを（クレジットカード、自動支払い、１日あたりの許可トークン購入数のいずれかによる）他のパラメータがチェックされる。

クレジットカードで支払いの場合、カードの番号は、ローカルブラックリストデータベース３２０５に記憶されたローカルブラックリストを基準にしてチェックされる。

検証の全てが成功した場合、ＡＳは、

１．請求書を生成し、この請求書を完全なものにし、それをファイルに記憶するＯＣＳに送る。このファイルは、後で、処理（顧客の実際の課金）のためにＳＭＳに送られる；および

２．主に新規の購入限界を設定するためにデータベースを更新する。

この「ＯＫならば請求書をチェックし生成する」機構は、加入者が単一接続中に要求できる各コマンドのために適用する（単一セッションの例えば５つの映画を注文することができる）。

ＡＳは、ＳＭＳによって保持される情報量と比較して、加入者に関する減少された情報量を有することに注目するべきである。例えば、ＡＳは、加入者の名前

あるいはアドレスを保持しない。一方では、ＡＳは、加入者のスマートカード番号、加入者の消費者カテゴリー（それで、異なるオファーは異なる加入者に対して行うことができる）、例えば、加入者がクレジットで購入できるか、あるいは加入者が資格を一時的に取り上げられるかあるいは加入者のスマートカードが盗まれたかどうかなどを示す様々なフラグを保持する。減少された情報量の使用は、特定の加入者要求を許可するのにかかる時間量を減少させるのに役立つことができる。

ＤＢＡＳ３２０６の主目的は、アクセスを平行させることによってＡＳから見たデータベース性能を増加させることにある（それで、実際、唯一のＤＢＡＳを有する配置を定義することはあまり意味がない）。ＡＳパラメータは、どれくらいの数のＤＢＡＳを接続すべきであるかを決定する。所与のＤＢＡＳは１つのＡＳに接続されてもよい。

ＯＣＳ２３０７は、主にＰＰＶコマンドを処理する。ＯＣＳ２３０７は、いくつかのモードで作動する。

まず第一に、ＯＣＳ２３０７は、製品リフレッシュメント（例えば、請求書がＳＭＳによって既に記憶されているならば、請求書はＯＣＳによって生成されない）、スマートカード３０２０におけるウォレットの更新、およびセッションキャンセル／更新のような、ＳＭＳによって出されたコマンドを処理するように作動する。

手順における様々なステップは、

１．関連加入者を（ＡＳ３２０２を使用して）識別すること；

２．有効の場合、適当なＥＭＭを送るためにメッセージ発生器に対する適切なコマンドを生成する。コマンドは、

製品コマンド、

ウォレットの更新、

セッション削除

であってもよい。

課金はＳＭＳから既に識別されるので、これらの操作は課金情報の作成を意味

しないことに注目すべきである。これらの操作は「無料製品」購入に適合される。

第二に、ＯＣＳは、通信サーバ３０２２を通して加入者から受信されたコマンドを処理する。これらは、受信機／デコーダ２０２０に接続されたモデムを介して、あるいは電話４００１を介する音声起動によって、あるいは使用可能な場合、ミニテル（ＭＩＮＩＴＥＬ）、プレステル（ＰＲＥＳＴＥＬ）、または同様なシステムを介するキー起動によってのいずれかで受信されてもよい。

第三に、ＯＣＳはＳＭＳによって発されたコールバックリクエストを処理する。これらの最後の２つの動作モードは次により詳細に述べられる。

前述の第２の種類のモードでは、ＯＣＳは、通信サーバ３０２２を通してエンドユーザ（加入者）から直接受信されたコマンドを処理することが示される。これらは、製品注文（例えば、特定のＰＰＶイベントのためのものである）、加入者によって要求された加入変更、および親コードのリセット（親コードは、親が所定のプログラムあるいはプログラムのクラスへのアクセス権利を制限できるコードである）を含む。

これらのコマンドが処理される方法は、次に図１１を参照してより詳細に述べられる。

加入者による製品注文は下記のステップを含んでいる。

１．ＣＳ３０２２を通して電話をかけ、特定の製品を注文する電話のかけ手をＡＳによって識別する。

２．ＡＳを再び使用して、電話のかけ手の要求妥当性をチェックすること（注文が受信機／デコーダ２０２０を使用して行われる場合、これはスマートカード３０２０細部を検証することによって実行される）。

３．購入の価格を確認する。

４．価格が電話のかけ手のクレジット制限等を超えないことをチェックする。

５．ＡＳからの部分請求書を受け取る。

６．完成された請求書を形成するために付加欄を請求書に記入する。

７．後処理のために完成された請求書を課金情報記憶ファイル３２１２に追加す

る。

８．対応するコマンドをＰＰＶメッセージ発生器３２１０に送り、関連ＥＭＭを生成する。

消費者が受信機／デコーダ２０２０（さらなるこの詳細は後述される）を使用して製品注文をした場合、ＥＭＭは、モデムライン４００２で送信されるかあるいは放送されるかのいずれかである。これの１つの例外は、モデム接続になんらかの障害がある場合である（消費者が受信機／デコーダを使用して注文をする場合）。すなわち、この場合、ＥＭＭは大気を介して放送される。

加入者によって要求された加入変更は下記を含む。

１．電話のかけ手を（ＡＳを使用して）識別すること

２．情報をコマンドインタフェースに送る；次に、ＣＩはこの情報をＳＭＳに転送する；および

３．ＣＩを通して、次に、ＯＣＳは、（変更が可能であるならば、変更のコストに関して）ＳＭＳからの回答を受信する。

変更が受信機／デコーダを使用して要求されるならば、ＯＣＳは、ＳＭＳの確認を発生する。さもなければ、例えば、電話あるいはミニテル(MINITEL)の場合、加入者は、確認のためにプロンプトされ、この回答は、ＯＣＳおよびＣＩを介してＳＭＳに送られる。

親コードのリセットは下記を含む。

１．電話のかけ手を（ＡＳを使用して）識別すること。および

２．コマンドをＭＧに送り、適当なリセットパスワードを含む適当なＥＭＭを発生する。

親コードのリセットの場合、コードをリセットするコマンドは、受信機／デコーダから生じることが許可されない安全理由のためである。ＳＭＳ、電話およびミニテル等だけがこのようなコマンドを生じ得る。したがって、この特定の場合、ＥＭＭは、決して電話回線でなく、大気でのみ放送される。

通信サーバがＳＡＳ、および特にＯＣＳに直接接続されているので、ユーザがＳＡＳ、および特にＯＣＳおよびＡＳへ直接アクセスすることができることがＯ

ＣＳの異なる動作モードの前述の例から理解される。この重要な特徴は、ユーザがユーザのコマンドをＳＡＳに通信する時間を減らすことに関している。

この特徴は、図１２をさらに参照して示されている。この図から、エンドユーザのセット・トップ・ボックス、および特に受信機／デコーダ２０２０は、ＳＡＳ３００２に関連した通信サーバ３０２２と直接通信する機能を有する。ＳＡＳ３００４を通るエンドユーザからＳＡＳ３００２の通信サーバ３０２２への接続の代わりに、この接続は直接ＳＡＳ３００２に対するものである。

実際、直接述べられているように、２つの直接接続が備えられる。

第１の直接接続は、エンドユーザが一連の音声コマンドあるいはコード番号をなお入力しなければならないが、ＳＭＳ３００４を介する通信と比較して時間が節約される電話４００１および適切な電話回線を介する音声リンク（および／または使用可能である場合、ミニテルあるいは同様な接続）によるものである。

第２の直接接続は、受信機／デコーダ２０２０からのものであり、データの入力は、自分自身のドータースマートカード３０２０を挿入するエンドユーザによって自動的に実行されるので、かかる時間およびこの入力を行う際のエラーの可能性を減らす関連データを入力しなければならないジョブからエンドユーザを解放する。

上記の論議から生じる他の重要な機能は、結果として生じるＥＭＭが、選択された製品のエンドユーザによって観察し始めるためにエンドユーザに送信されるのにかかる時間を減らすことに関する。

広義の用語において、図１２を参照すると、この機能は、再度、ＳＡＳ３００２に関連した通信サーバ３００２と直接通信する機能をエンドユーザの受信機／

デコーダ２０２０を与えることによって実行される。

前述のように、複合受信機／デコーダ２０２０は、モデムバックチャネル４００２によって通信サーバ３０２２に直接接続されるので、デコーダ２０２０からのコマンドは、ＳＡＳ３０２２によって処理され、（ＥＭＭを含む）メッセージが生成され、それからバックチャネル４００２を通してデコーダ２０２０に直接送り返される。プロトコルは、ＣＳ３０２２と受信機／デコーダ２０２０との間

の通信に使用されるので（後述される）ＣＳは、関連ＥＭＭの受信肯定応答を受信し、それによってこの手順に確実性を加える。

したがって、例えば、プレブックモードの場合、ＳＡＳ３００２は、エンドユーザからスマートカード・デコーダ２０２０を介してそのモデムおよび電話回線４００２を介してメッセージを受信し、特定のイベント／製品へのアクセスを要求し、適当なＥＭＭを電話回線４００２およびモデムを介してデコーダ２０２０に戻す。このモデムおよびデコーダは、セット・トップ・ボックス（ＳＴＢ）に一緒に置かれることが好ましい。

したがって、これは、エンドユーザがイベント／製品を見ることができるようにマルチプレクサ・スクランブラ２００４、アップリンク２０１２、衛星２０１４およびデータリンク２０１６を介してＭＰＥＧ－２データストリーム２００２におけるＥＭＭを送信する必要なく達成される。これは時間およびバンド幅に関してかなり節約できる。加入者が自分の買物のために支払うや否や、ＥＭＭは受信機／デコーダ２０２０に到達する実際上の確実性がもたらされる。

前述のＯＣＳ３２０７の第３のタイプの動作モードにおいて、ＯＣＳはＳＡＳによって出されたコールバックリクエストを処理する。これは図１３に関して示される。典型的なコールバックリクエストは、ＳＡＳが受信機／デコーダに要求する情報とともに、ＳＡＳを受信機／デコーダ２０２０がモデムバックチャネル４００２を介してコールバックすることを確実にする目的を有する。

コマンドインタフェース３１０２によって命令されるように、加入チェーンメッセージ発生器３１０６は、コールバックＥＭＭを生成し、受信機／デコーダ２０２に送信する。

このＥＭＭはセキュリティの理由で暗号化装置３００８によって暗号化される。

受信機／デコーダが明確に要請されないで、コールバックを単独で起動し、実行すべきである時間／日付をＥＭＭは含んでもよい。すなわち、ＥＭＭはまた、一般的には、端末がダイヤルしなければならない電話番号、失敗した呼び出しの後の他の試みの数および２つの呼び出しの間の遅れを含んでもよい。

ＥＭＭを受信する場合、あるいは特定の時間－日付で、受信機／デコーダは通信サーバ３０２２に接続する。ＯＣＳ３２０７は、ＡＳ３２０２を使用して電話のかけ手を最初に識別し、スマートカードオペレータおよび加入者詳細のような所定の詳細を検証する。

次に、ＯＣＳは、様々な暗号化情報（例えば、関連セッション数、いつセッションが観察されるか、何回加入者が再びセッションを見るために許可されるか、セッションが観察される方法、残りのトークン数、プレブックセッション数等）を送信するようにスマートカード３０２０に要求する。この情報は、再び暗号化装置３００８を使用して、ＰＰＶチェーンメッセージ生成器３２１０によって暗号解読される。

ＯＣＳは、後で処理し、ＳＭＳ３００４に送るためにこの情報をコールバック情報記憶ファイル３２１４に追加する。この情報はセキュリティ理由のために暗号化される。全手順は、スマートカードから読み取られる以上の何物でもなくなるまで繰り返される。

コールバック機構の１つの特定の好ましい機能は、スマートカードを読み取る前（前述のようにＡＳ３２０２を使用して電話のかけ手の識別直後）、受信機／デコーダが海賊版あるいはコンピュータシミュレーションよりもむしろ本当に本物であるかのチェックがＳＡＳ３００２によって行われることである。このようなチェックは下記のように実行される。ＳＡＳは、受信機／デコーダによって受信され、暗号化され、それからＳＡＳに戻される乱数を生成する。ＳＡＳはこの数を暗号解読する。暗号解読が成功し、元の乱数が引き出されるならば、受信機／デコーダが本物であると決定され、手順が続く。さもなければ、手順が中止される。

コールバック中に生じる得る他の機能は、スマートカードのもはや使用されていないセッションの削除あるいはウォレットの充てんである（これは後で、「スマートカード」というタイトルの節の下で後述される）。

さらに、ペイ・パー・ビューチェーン領域３２００に関して、通信サーバ３０２２の説明が次に行われる。ハードウェアレベルで、これらは、ＤＥＣの４つの

並列プロセッサマシンを備えている。ソフトウェアアーキテクチャレベルで、図１４を参照すると、多数の点で通信サーバは通常のものである。従来の設計からの１つの特別の逸脱は、サーバが受信機／デコーダ２０２０および従来の電話４００１、多分ミニテルあるいは同様なシステムをも有する音声通信の両方に役立つという事実から生じる。

送る際に、２つの注文集中化サーバ３２０７が（「ＯＣＳ１」および「ＯＣＳ２」のように）図１４に示されることが注目される。当然、任意の所望の数が与えられてもよい。

通信サーバは、２つの主サーバ（「ＣＳＵおよび「ＣＳ２」）ならびに多数のフロンタルサーバ（「フロンタル１」および「フロンタル２」）を含む。すなわち、２つのフロンタルサーバが図に示されているが、一般的には、主サーバ毎に１０あるいは１２が備えられてもよい。

確かに、２つの主サーバＣＳ１およびＣＳ２および２つのフロンタルサーバ、フロンタル１およびフロンタル２が示されているけれども、任意の数を使用できる。何らかの冗長性は通常望ましい。

ＣＳ１およびＣＳ２は、高レベルＴＣＰ／ＩＰリンク３２３０を介してＯＣＳ１およびＯＣＳ２に結合されるのに対して、ＣＳ１およびＣＳ２は、他のＴＣＰ／ＩＰリンクを介してフロンタル１およびフロンタル２に結合されている。

図示されるように、ＣＳ１およびＣＳ２は、「ＳＥＮＤＯＲ」（送信）、「ＲＥＣＶＲ」（受信）、「ＶＴＸ」（ミニテル、プレステル等）、「ＶＯＸ」（音声通信）、および「ＴＲＭ」（受信機／デコーダとの通信）のためのサーバを備えている。これらは、フロンタルサーバへの信号の通信のために「ＢＵＳ」に結合されている。

ＣＳ１およびＣＳ２は、Ｘ２５公衆ネットワーク共通プロトコルを使用してそのモデムバックチャネル４００２を介して受信機／デコーダ２０２０と直接通信する。通信サーバ３０２２と受信機／デコーダ３０２０との間の比較的低いレベルのプロトコルは、１つの好ましい実施例では、Ｖ４２標準国際ＣＣＩＴＴプロトコルに基づいている。このＶ４２標準国際ＣＣＩＴＴプロトコルは、エラー検

出機構およびデータ再伝送機構を有することによって信頼性をもたらし、再伝送の完全性をチェックするためにチェックサムルーチンを使用する。エスケープ機構も、不許可文字の伝送を防止するために備えられる。

一方、音声電話通信は、各々が、高速「Ｔ２」（Ｅ１）標準電話通信システムのＩＳＤＮ回線を介して接続部３２３４からローカル電話ネットワークへの約３０の同時音声接続を続けることができるフロンタル通信サーバを介して実行される。

通信サーバのソフトウェア部の３つの特定の機能（もちろん、その代わりにハードウェアで十分実現できる）は、まず第一に受信機／デコーダから受信された比較的低いレベルのプロトコル情報をＯＣＳへの比較的高いレベルのプロトコル情報に変換することにあり、第二に、行われた同時接続の数を減じるかあるいは制御することにあり、第三に、混合せずにいくつかの同時チャネルを備えることにある。この最後の点では、通信サーバは実際、通信チェーン中に使用される、所与のセッションＩＤ（識別子）によって規定されている特定のチャネルにおける対話に関してマルチプレクサの形式の役割を演じる。

最後に、ペイ・パー・ビューチェーン領域３２００に関しては、再び、図５を参照すると、プログラム放送のためのサーバ（ＳＰＢ）３２０８は、１つあるいはそれ以上のプログラム放送器３２５０（一般的には、ＳＡＳから離れて置かれる）に結合され、プログラム情報を受け取る。ＳＰＢは、ＰＰＶイベント（セッション）に対応する情報を他の使用のためにフィルタリング出力する。

特に重要な機能は、フィルタリングプログラムイベント情報がＳＰＢによってＭＧに送られることであり、このＭＧは同様に指令（制御コマンド）をＭＥに送信し、ＥＭＭの周期的放出の速度を所与の状況で変える。すなわち、これは、関連セッション識別子を有する全てのＥＭＭを検出し、このようなＥＭＭに割り当てられたサイクル速度を変えるＭＥによって行われる。

この機能は特定のＥＭＭに対するバンド幅の動的割り当てとみなすことができる。周期的ＥＭＭ放出は、ＥＭＭインジェクタに関連して下記の節でより詳細に検討される。

サイクル速度が変えられる状況は、次に図１５を参照して述べられる。この図１５は、特定のＰＰＶプログラムイベント前からイベントの終了までの短い期間（約１０分）、いかにサイクル速度３２５２が、これらの時間にＰＰＶイベントに対する予想される余分のユーザ要求を満たすために３０分毎に約１回の遅いサイクル速度から３０秒～１分毎に約１回の速いサイクル速度に上昇されるかを示している。このように、バンド幅は予想されるユーザ要求により動的に割り当てることができる。これは全バンド幅要求を減らすことを助けることができる。

他のＥＭＭのサイクル速度は変更することもできる。例えば、加入ＥＭＭのサイクル速度は、適切なビットレート指令を送信するマルチプレクサ・スクランブラ２００４によって変更できる。

ＥＭＭインジェクタ

ＥＭＭインジェクタ３３００に関しては、ＥＭＭインジェクタの一部を形成し、メッセージ生成器のための出力手段としての役目を果たすメッセージ放出器３３０２～３３０８の詳細は、次に図１６を参照して述べられる。その機能は、ＥＭＭを処理し、これをそれぞれのリンク３３１４および３３１６を介してソフトウェアマルチプレクサ３３１０および３３１２に、それからハードウェアマルチプレクサ・スクランブラ２００４に周期的に（カルーセルの方法で）送ることにある。応答において、ソフトウェアマルチプレクサ・スクランブラ２００４は、グローバルビットレート指令を生成し、ＥＭＭの全サイクリング速度を制御する。そうするために、ＭＥは、サイクル時間、ＥＭＭのサイズ等のような様々なパラメータを考慮する。この図において、ＥＭＭ＿ＸおよびＥＭＭ＿Ｙは、演算子ＸおよびＹに対するグループＥＭＭであるのに対して、ＥＭＭ＿Ｚは、演算子Ｘあるいは演算子Ｙのいずれかに対する他のＥＭＭである。

更なる説明はメッセージ放出器の中の典型的なメッセージ放出器に対して進める。すなわち、残りのＭＥが同様に作動することが理解される。ＭＥは、ＭＧからの指令の制御の下で、ＥＭＭがＰＰＶ　ＥＭＭであるならば、最も著しい送信開始・停止時間および放出速度、ならびにセッション数を操作する。放出速度に関して、好ましい実施例では、関連指令は、非常に速いから非常に遅いまでの５

つの値の中から１つを処理してもよい。数値が指令で特定されるのではなく、むしろＭＥが、指令をＳＡＳの関連部分によって供給される実際の数値にマッピングする。好ましい実施例では、５つの放出速度は下記の通りである。

１．非常に速い　－毎３０秒
２．速い　－毎分
３．中間　－毎１５分
４．遅い　－毎３０分
５．非常に遅い　－毎３０分

ＭＥは、第１および第２のデータベース３３２０および３３２２を有する。第１のデータベースは、その放送日付をまだ達成していないこれらのＥＭＭのためのものである。すなわち、これらは一連の年代順ファイルをデータベースに記憶されている。第２のデータベースは、中間放送用ＥＭＭのためのものである。

システムクラッシュの場合、ＭＥは、関連記憶ファイルを再読み出し、正しい放送を実行する能力を有するように構成されている。データベースに記憶された全てのファイルは、ＭＥが入来指令とＭＥに既に送信されたＥＭＭとの間の整合性を保持することを望む場合、ＭＧからの要求と同時に更新される。実際放送されているＥＭＭはランダムアクセスメモリ３３２４にも記憶される。

メッセージ生成器におけるＦＩＦＯ３１６２および３１６４およびメッセージ放出器におけるデータベース３３２０および３３２２の組み合わせは、これらの２つの間のリンク３１６６が一時的に遮断される場合、２つがスタンドアロンで作動できることを意味する。

ソフトウェアマルチプレクサ（ＳＭＵＸ）３３１０および３３１２は、ＭＥとハードウェアマルチプレクサ２００４との間にインタフェースを与える。好ましい実施例では、一般に１つのＳＭＵＸと接続することができるＭＥの数には制限がないけれども、ソフトウェアマルチプレクサ（ＳＭＵＸ）３３１０および３３１２の各々はＭＥの中の２つからＥＭＭを受信する。ＳＭＵＸは、ＥＭＭを集中し、それからこのＥＭＭをＥＭＭの種類に従って適切なハードウェアマルチプレクサに送る。ハードウェアマルチプレクサは異なる種類のＥＭＭを受け入れ、こ

れらをＭＰＥＧ－２ストリームの異なる位置に配置するためにこれは必要である。ＳＭＵＸもハードウェアマルチプレクサからのグローバルビットレート指令をＭＥに転送する。

ＭＥの１つの特定の重要な機能は、ＭＥがランダム順序でＥＭＭを放出することにある。このための理由は下記の通りである。メッセージ放出器は、マルチプレクサに放出することを検出するかあるいは制御する能力を全く有しない。したがって、メッセージ放出器は連続して受信機／デコーダ２０２０によって受信され、復号化されるべき２つのＥＭＭを送信できる可能性がある。

このような状況では、さらに、ＥＭＭが十分分離されない場合、受信機／デコーダおよびスマートカードがＥＭＭの中の二番目を検出し、適切に復号化できない可能性がある。周期的にＥＭＭをランダム順序に放出することでこの問題は解決できる。

ランダム化が実行される方法は、次に図１７に関して述べられる。好ましい実施例では、必要なソフトウェアロジックはＡＤＡコンピュータ言語で実行される。ランダム化の特別の重要な部分は、データベース３３２０および３３２２（バックアップ目的のために使用される）およびＲＡＭ３３２４へのＥＭＭの正しい記憶である。

特定のサイクル速度およびオペレータに関しては、ＥＭＭは、列３３３０（例えば、ＡからＺに進む）および列３３３２における数（０からＮまで進む）によって２次元アレイに記憶される。第３の次元は、サイクル速度３３３４によって追加されるので、サイクル速度と同じ数の２次元アレイがある。好ましい実施例では、２５６列があり、一般的には各列には２００あるいは３００のＥＭＭがある。すなわち、５サイクル速度がある。アレイの最終次元は異なるオペレータの存在によって追加される。つまりオペレータと同じ数の３次元アレイがある。この方法でのデータの記憶は、ＭＧが特定のＥＭＭを削除したい場合、迅速な検索を可能にできる。

ＥＭＭの記憶は、「ハッシュ」アルゴリズム（特に、「一方向ハッシュ関数」として既知である）により行われる。これはモジュロ方式で操作するので、連続

列は、列におけるより高い数が使用される前に満たされ、各列におけるＥＭＭの数は、概ね一定のままである。この例は２５６の列があるものとみなされる。ＭＧが識別子（ＩＤ）１を有するＥＭＭをＭＥに送信する場合、列「１」は、このＥＭＭに割り当てられ、列３３３０において最初の数３３３２を受け入れる。

ＩＤ２を有するＥＭＭは列「２」に割り当てられ、列２５６まで同様に割り当てられる。ＩＤ２５７を有するＥＭＭは、（モジュロ機能に基づいて）列「１」に再度割り当てられ、第１の列における第２の数を受け入れ、以下同様にする。

例えば、特定のＥＭＭの削除がＭＧによって要求される場合、特定のＥＭＭの検索は上記の逆のことによって行われる。ハッシュアルゴリズムは、列を得るために列における数がその後に検出されるＥＭＭ　ＩＤに適用される。

実際のランダム化は、ＥＭＭがメッセージ放出器のハードウェアおよび／またはソフトウェアで実行されるランダム化手段３３４０を使用して周期的にＲＡＭ３３２４から検索される。検索はランダムであり、再びハッシュアルゴリズムに基づいている。

まず第一に、乱数（上記の例においては最初は１～２５６の範囲にある）は列における特定の数を生じるように選択される。第二に、他の乱数は列において特定の数を生じるように選択される。他の乱数は、所与の列におけるＥＭＭの全数によりＥＭＭの全数により選択される。所与のＥＭＭが選択され、放送されると、ハッシュ関数を再び使用してＲＡＭ３３２４における第２の同一の記憶領域に移動される。

したがって、第１の領域は、ＥＭＭが放送されると、サイズが、一旦全列が使用されると、これが削除される程度まで減少する。一旦第１の記憶領域が完全に空になると、第１の記憶領域は、新しいＥＭＭ放送の循環前に第２の記憶領域と取り替えられ、またその逆も行われる。

上記のように、ＥＭＭの２サイクルあるいは３サイクルの後、統計的には、連続して送信される同じエンドユーザに対して望まれる任意の２つのＥＭＭの可能性は無視できる。

ＥＭＭが記憶されている一定の間隔で、コンピュータ３０５０は、記憶装置に

おけるバイト数を計算し、これから、マルチプレクサおよびソフトウェアマルチプレクサからのグローバルビットレート指令を与えた放出のビットレートを計算する。

バックアップデータベース３３２０および３３２２に対する参照は上記で行われた。実際、好ましい実施例では、ＲＡＭ３３２４の中にあるもののバックアップバージョンを保持するシーケンシャルファイルメモリがある。メッセージ放出器の故障およびその後の再始動の場合、あるいはより一般的にはＭＥが如何なる理由でも再始動される場合、それを介して記憶されたＥＭＭがＲＡＭにアップロードされるリンクがＲＡＭとデータベースとの間に形成される。このように、故障の場合、ＥＭＭを失う危険を取り除くことができる。

列が一般的には所与のオペレータに対応し、列における数がセッション数に対応する場合、ＰＰＶ　ＥＭＭの同様な記憶は、加入ＥＭＭに関しては前述の記憶装置に生じる。

スマートカード

ドーター、すなわち「加入者」のスマートカード３０２０は、図１８に概略的に示され、使用中受信機／デコーダ２０２０のカードリーダーの対応する接点のアレイに接続される接点の標準アレイ１２０に結合される入出力バスを有するモトローラ６８０５マイクロプロセッサのような８ビットマイクロプロセッサ１１０を備え、カードリーダーは従来の設計のものである。マイクロプロセッサ１１０には、好ましくはマスクＲＯＭ１３０、ＲＡＭ１４０およびＥＥＰＲＯＭ１５０に対するバス接続部も装備されている。

スマートカードは、スマートカードの所定の物理的パラメータ、チップ上の接点の位置および外部システム（および特に受信機／デコーダ２０２０）とスマートカードとの間での所定の通信をそれぞれ決定するので、ここではさらに説明されないＩＳＯ７８１６－１、７８１６－２および７８１６－３の標準プロトコルに従う。マイクロプロセッサ１１０の１つの機能は、次に述べられるようにスマートカードのメモリを管理することにある。

ＥＥＰＲＯＭ１５０は、所定の動的に作成されるオペレータゾーン１５４、１５５、１５６および次に図１９を参照して述べられる動的に作成されたデータゾ

ーンを含んでいる。

図１９を参照すると、ＥＥＰＲＯＭ１５０は、スマートカード３０２０の製造者によって設定される固定加入者スマートカード識別子を含む８バイトの固定「カードＩＤ」（すなわち製造者）ゾーン１５１を備えている。

スマートカードがリセットされる場合、マイクロプロセッサ１１０は、受信機／デコーダ２０２０に信号を出す。この信号は、スマートカードによって使用される条件付アクセスシステムの識別子およびカードＩＤを含むスマートカードに記憶されたデータから発生されたデータを含む。この信号は、スマートカードが受信機／デコーダ２０２０によって使用された条件付アクセスシステムとコ適合性があるかを検査するために記憶信号をその後に使用する受信機／デコーダ２０２０によって記憶される。

ＥＥＰＲＯＭ１５０は、擬似乱数を発生するプログラムを含む固定「乱数発生器」ゾーン１５２も含んでいる。このような乱数は、スマートカード３０２０によって発生されたトランザクション出力信号をさまさまざまに変化させるために使用され、放送器に送り返される。

乱数発生器ゾーン１５２の下に１４４バイトの固定「管理」ゾーン１５３が装備される。固定管理ゾーン１５３は、後述されるようにゾーン１５４、１５５、１５６･･･の動的作成（および除去）においてＲＯＭ１３０のプログラムによって利用される特定のオペレータゾーンである。

固定管理ゾーン１５３は、ゾーンを作成あるいは取り除くスマートカードの権利に関するデータを含んでいる。

ゾーンを動的に作成し、取り除くためのプログラムは、ＳＡＳ３００２によって送信され、受信機／デコーダ２０２０によって受信され、加入者スマートカード３０２０に送られる特定のゾーン作成（あるいは除去）ＥＭＭに応答する。ＥＭＭを作成するために、オペレータは管理ゾーンに専用の特定キーを必要とする。これは一人のオペレータが他のオペレータに関するゾーンを削除することを防止する。

管理ゾーン１５３の下には、オペレータ１、２････Ｎのそれぞれに対する一連の「オペレータＩＤ」ゾーン１５４、１５５、１５６がある。通常、少なくとも

１つのオペレータＩＤゾーンは、エンドユーザがこのオペレータによって放送されるプログラムを暗号解読することができるように加入者スマートカード３０２０のＥＥＰＲＯＭにプリロードされる。しかしながら、他のオペレータＩＤゾーンは、その後に述べられるように、エンドユーザ（加入者）によって自分のスマートカード３０２０を介して発生されたトランザクション出力信号に応じて管理ゾーン１５３を使用してその後に動的に作成できる。

各オペレータゾーン１５４、１５５、１５６は、スマートカード３０２０が属するグループの識別子およびグループ内部のスマートカードの位置を含んでいる。このデータは、スマートカードが（そのグループにおける他のスマートカードとともに）このグループのアクセスを有する（がグループにおけるスマートカードの位置でない）放送「グループ」加入ＥＭＭならびにグループ内部のこのスマートカードにのみアドレス指定される「個人」（あるいは商業オファー加入）ＥＭＭに応答することを可能にする。各々のこのようなグループの２５６のメンバースマートカードがある可能性があるので、この機能はＥＭＭを放送するのに必要なバンド幅を著しく減少させる。

「グループ」加入ＥＭＭを放送するのに必要なバンド幅をさらに減らすために、スマートカード３０２０および他のドータースマートカードのＥＥＰＲＯＭにおける各オペレータゾーン１５４、１５５、１５６、および全ての同様なゾーンにおけるグループデータは、例えば、グループのメンバーの削除によって作成された任意の穴を満たすように各グループにおけるその位置を特定のスマートカードができるように連続して更新される。この穴は、ＳＴＭサーバ３１０４においてこのような穴のリストがある場合、ＳＡＳ３００２によって満たされる。

このように、断片化が減少され、各グループのメンバーシップは、２５６人のメンバーの最大にあるいはその近くに保持される。

各オペレータゾーン１５４、１５５、１５６は、ＥＥＰＲＯＭ１５０に記憶された１つあるいはそれ以上の「オペレータデータオブジェクト」に関連している。図１９に示されるように、一連の動的に作成された「オペレータデータ」オブジェクト１５７～１６５はオペレータＩＤゾーンの下に置かれる。これらのオブジェクトの各々は下記のａ）、ｂ）、ｃ）でラベル付けされる。

ａ）図１９の左側部に示されるように関連オペレータ１，２，３･･･Ｎに対応する「識別子」１，２，３･･･Ｎ

ｂ）オブジェクトのタイプを示す「ＩＤ」

ｃ）図１９の各関連オペレータオブジェクトの右側部に示されるようにデータのために用意された「データ」ゾーン。オペレータ１のデータオブジェクトにおけるデータのタイプの下記の説明が全て他のオペレータのデータオブジェクトにも適用可能であるように各オペレータは同様なデータオブジェクトのセットに関連することを理解すべきである。さらに、データオブジェクトは、ＥＥＰＲＯＭの隣接する物理的領域に置かれ、その順序は重要てない。

データオブジェクトの削除は、スマートカードに穴１６６を形成する、すなわち、削除されたオブジェクトが予め占有されるバイト数は直ちに占有されない。

このように「自由された」バイト数、すなわち「穴」は下記でラベル付される。

ａ）「識別子」０、および

ｂ）　バイトがオブジェクトを自由に受け取ることができることを示す「ＩＤ」

作成された次のデータオブジェクトは、識別子０によって識別されるような穴を満たす。このように、ＥＥＰＲＯＭ１５０の限られたメモリ容量（４キロバイト）は有効に利用される。

次に、各オペレータに関連するデータのセットに向けると、データオブジェクトの例が次に述べられる。

データオブジェクト１５７は、受信機／デコーダ２０２０によって受信された暗号化ＥＭＭを暗号解読するために使用されるＥＭＭキーを含んでいる。このＥＭＭキーはデータオブジェクト１５７に永久記憶されている。このデータオブジェクト１５７は、スマートカード３０２０の配布前に作成されてもよいし、および／または（前述のように）新しいオペレータゾーンを作成する場合、動的に作成されてもよい。

データオブジェクト１５９は、エンドユーザが加入した特定のプログラムの「ブーケ」を暗号解読することができるように関連オペレータ（この場合、オペレータ１）によって送信される。新しいＥＣＭキーは、（この場合）オペレータ

１からの放送を見るエンドユーザの全権利を更新するグループ加入（更新）ＥＭＭとともに、一般的には毎月送信される。

別々のＥＭＭキーおよびＥＣＭキーの使用は、見る権利が異なる方法で（この実施例では、加入によりおよび個別的に（ペイ・パー・ビュー））購入することを可能にし、セキュリティも増加する。このペイ・パー・ビュー（ＰＰＶ）モードはその後に述べられている。

新しいＥＣＭキーは周期的に送られるので、例えば、受信機／デコーダをスイッチオフするかあるいはクロックをリセットし、受信機／デコーダ２０２０のタイマが無効できるように古いＥＣＭキーの満了を防止することによってユーザが古いＥＣＭキーを使用することを防止することが重要である。したがって、オペレータゾーン１５４は、ＥＣＭキーの陳腐化日付を含む領域（一般的には２バイトのサイズを有する）を含んでいる。スマートカード３０２０は、この日付と受信ＥＣＭに含まれる現日付とを比較し、現日付が陳腐化日付よりも後である場合、暗号解読を防止するように構成されている。陳腐化日付は、前述のようにＥＭＭを介して送信される。

データオブジェクト１６１は、加入者が加入した放送オペレータのプログラムの正確な表示である６４ビット加入ビットマップを含む。あらゆるビットは、プログラムを示し、プログラムが加入されている場合、「１」をセットし、プログラムが加入されていない場合、「０」をセットする。

データオブジェクト１６３は、例えば、無料プリビューあるいは他の宣伝に応じて当面の放送を見る権利を買うためにＰＰＶモードで消費者によって使用することができる多数のトークンを含んでいる。データオブジェクト１６３は、消費者に対するクレジットを可能にするために例えば負の値をセットされてもよい限界値も含む。トークンは、例えば、クレジットによって、およびモデムバックチャネル４００２を介して、あるいは例えばクレジットカードと組み合わせて音声サーバを使用することによって購入することができる。特定のイベントは１つのトークンあるいは多数のトークンとして代金を請求できる。

データオブジェクト１６５は、図２０のテーブル１６７に関して示されるように、ＰＰＶイベントの記述を含んでいる。

ＰＰＶイベント記述１６７は、視聴セッションを識別する「セッションＩＤ」１６８（プログラムおよび放送の時間や日付に対応する）と、いかに視聴権が購入されるかを示す「セッションモード」１６９（例えば、プレブックモードにおいて）と、「セッションインデックス」１７０と、「セッションビュー」１７１とを含んでいる。

プログラムをＰＰＶモードで受信することに関して、受信機デコーダ２０２０は、プログラムがＰＰＶモードで販売されたプログラムであるかどうかを決定する。そうであるならば、デコーダ２０２０は、プログラムのためのセッションＩＤがそれに記憶されているかどうかをＰＰＶイベント記述１６７に記憶された項目を使用してチェックする。セッションＩＤがそこに記憶されているならば、制御語がＥＣＭから抽出される。

セッションＩＤがそこに記憶されていない場合、特定のアプリケーションによって、受信機／デコーダ２０２０は、エンドユーザがＥＣＭから読み取られるように約２５トークンのコストでセッションを見るかあるいはイベントを購入するために通信サーバ３０２２に接続する権利を有することを示すメッセージをエンドユーザに表示する。

トークンを使用して、エンドユーザが（遠隔コントローラ２０２６によって（図２を参照））「イエス」と答えるならば、デコーダ２０２０は、ＥＣＭをスマートカードに送信し、スマートカードは、２５トークンだけスマートカード３０２０のウォレットを減らし、ＰＰＶイベント記述１６７におけるセッションＩＤ１６８、セッションモード１６９、セッションインデックス１７０およびセッションビュー１７１を書き込み、ＥＣＭから制御語を抽出し、この制御語を暗号解読する。

「プレブック」モードでは、ＥＭＭはスマートカード３０２０に送られるので、スマートカードは、ＥＭＭを使用してＰＰＶイベント記述１６７におけるセッションＩＤ１６８、セッションモード１６９、セッションインデックス１７０およびセッションビュー１７１を書き込む。

セッションインデックス１７０は、一方の放送と他方の放送とを区別するようにセットできる。この機能は、許可が放送のサブセットに対して、例えば、５つ

の放送の中の３回を与えることを可能にする。ＰＰＶイベント記述１６７に記憶された現セッションインデックス１７０とは異なるセッションインデックスを有するＥＣＭがスマートカードに送られるや否や、セッションビュー１７１の数は１だけ減らされる。セッションビューがゼロに達する場合、スマートカードは、現セッションインデックスに対して異なるセッションインデックスを有するＥＣＭを暗号解読することを拒否する。

セッションビューの初期値は、放送供給者が、関連するイベントを規定することを望む方法によってだけ決まる。すなわち、それぞれのイベントに対するセッションビューは任意の値をとってもよい。

スマートカードのマイクロプロセッサ１１０は、何時特定のプログラムの視聴数に対する制限に達したかを検出するために計数および比較プログラムを実行する。

ＰＰＶイベント記述１６７におけるセッションＩＤ１６８、セッションモード１６９、セッションインデックス１７０およびセッションビュー１７１は、前述のように「コールバック」手順を使用してスマートカードから抽出されてもよい。

各受信機／デコーダ２０２０は、この受信機／デコーダを独自に識別するかあるいはその製造者を識別するかのいずれかを行うことができるか、あるいは受信機／デコーダが特定の個人スマートカード、同じ製造者あるいは対応する製造者によって作られた特定の種類のスマートカード、この種の受信機／デコーダと排他的に併用することを目的としている任意の他の種類のスマートカードとだけ作動できるように他の方法で受信機／デコーダを分類できる識別子を含む。このように、１放送供給者によって消費者に供給された受信機／デコーダ２０２０は、非許可ドータースマートカード３０２０の使用から守られる。

さらに、またスマートカードと受信機の間にあるこの最初の「ハンドシェーク」の代わりに、スマートカード３０２０のＥＥＰＲＯＭは、スマートカードが機能を果たすことができる受信機／デコーダ２０２０のカテゴリーを記述するフィールドあるいはビットマップを含むことができた。これらは、スマートカード３０２０の製造中あるいは特定のＥＭＭによってのいずれかで特定できた。

スマートカード３０２０に記憶されたビットマップは、各々にスマートカードが使用されてもよいように対応する受信機／デコーダＩＤで識別される８０までの受信機／デコーダのリストを一般的に含んでいる。各受信機／デコーダに関連するのは、スマートカードが受信機／デコーダと併用できるか否かを示すレベル「１」あるいは「０」である。受信機／デコーダのメモリ２０２４のプログラムは、スマートカードに記憶されたビットマップにおける受信機／デコーダの識別子を検索する。識別子が検出されるならば、識別子に関連した値は「１」であり、それからスマートカードは使用可能にされる。検出されないならば、スマートカードは受信機／デコーダとともに機能を果たさない。

さらに、一般的には、オペレータ間の合意のために、特定の受信機／デコーダにおける他のスマートカードの使用を許可することが望まれる場合、特定のＥＭＭはトランスポンダ２０１４を介してそのビットマップを変えるためにこれらのスマートカードに送られる。

各放送供給者は、ある種の所定の判定基準により自分の加入者を区別できる。例えば、多数の加入者は「ＶＩＰ」として分類できる。したがって、各放送供給者は自分の加入者を複数のサブセットに分類でき、各サブセットは任意の加入者数を含む。

特定の加入者が属するサブセットはＳＭＳ３００４にセットされる。次に、ＳＡＳ３００２は、加入者がスマートカードのＥＥＰＲＯＭの約１５４の関連オペレータデータゾーンの中に属するサブセットに関する情報（一般的には１バイトの長さ）を書き込む加入者に送信する。次に、イベントが放送供給者によって放送されると、一般的には２５６ビットのＥＣＭは、イベントとともに送信され、加入者のサブセットのどれがイベントを見ることができるかを示している。オペレータゾーンに記憶された情報により、加入者がＥＣＭによって決定されるようにがイベントを見る権利を有していない場合、プログラム視聴が否定される。

この機能は、例えば、特定のプログラム、特に、特定の地理的な地域で行われるスポーツ競技種目に関するプログラムの送信中特定の地理的な地域での所与のオペレータのスマートカードの全てをスイッチオフするために使用されてもよい

。このように、フットボールクラブおよび他のスポーツ団体は、その場所以外の放送権を販売できると同時に地方のスポーツのサポーターがテレビでこの競技種目

を見ることを防止する。このように、地方のサポーターは、チケットを買い、スポーツ競技種目に参加するように勧められる。

ゾーン１５１～１７２に関連した機能の各々は、ゾーンの動的作成とは無関係の別個の発明とみなされる。

本発明は、単に例として述べられ、詳細の変更は本発明の範囲内で行うことができる。

説明に開示された各特徴、および（妥当である場合）請求の範囲および図面は、別々にあるいは任意の適切な組み合わせで提供されてもよい。

前述の好ましい実施例では、本発明のある種の特徴はコンピュータソフトウェアを使用して実現された。しかしながら、もちろん、これらの特徴のいずれかはハードウェアを使用して実現されてもよいことは当業者に明らかである。さらに、ハードウェア、コンピュータソフトウェア等によって実行された機能は、電気信号等であるいは電気信号を使用して実行されることは容易に理解される。

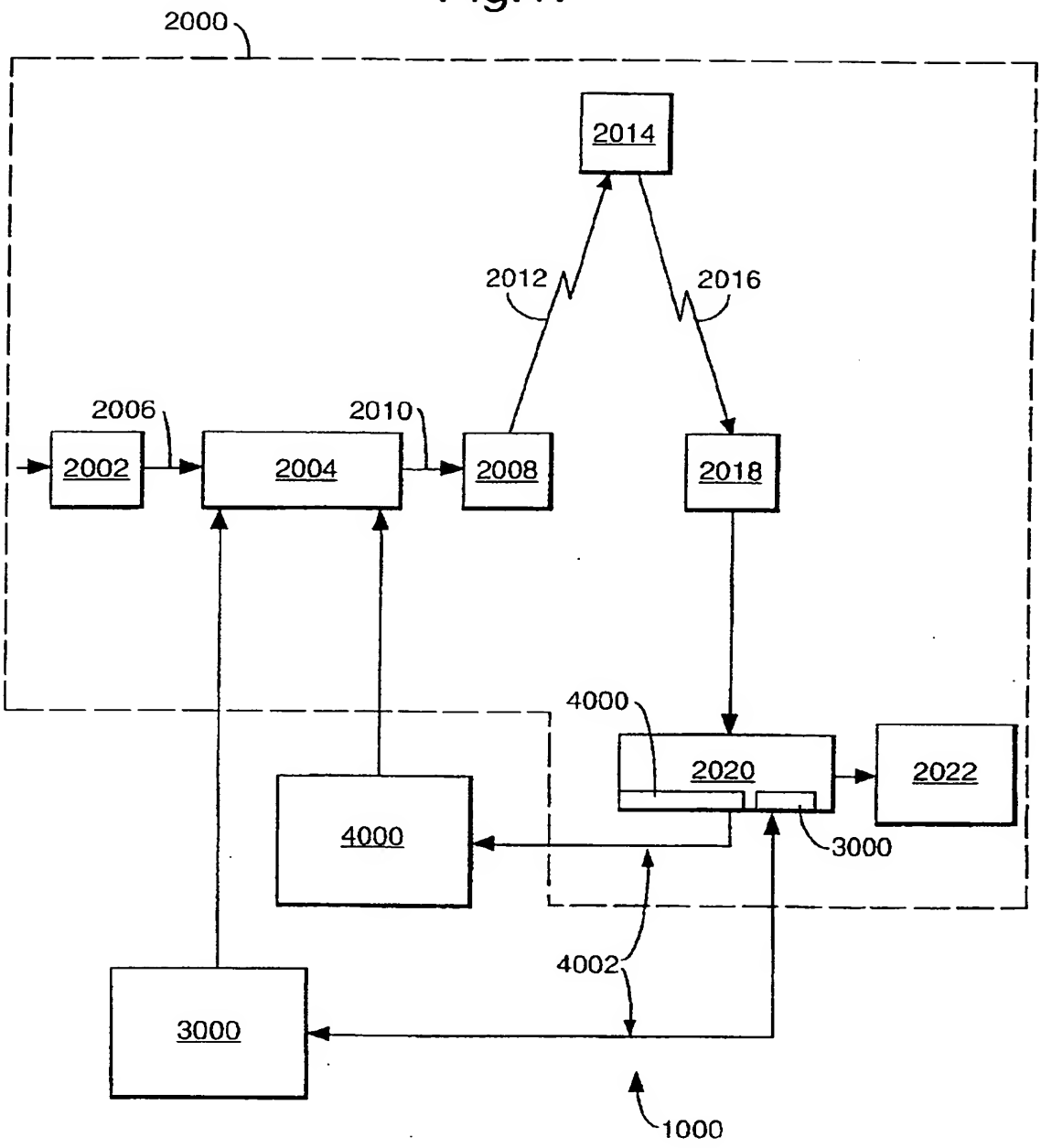
相互参照は、我々の同時係属出願に対して行われ、全ては、同じ出願日を有し、名称が「信号発生および放送（代理人参照番号ＰＣ／ＡＳＢ／１９７０７）」、「暗号化放送信号の受信機と併用するためのスマートカード、および受信機（代理人参照番号ＰＣ／ＡＳＢ／１９７０８）」、「放送・受信システムおよびそのための条件付アクセスシステム（代理人参照番号ＰＣ／ＡＳＢ／１９７１０）」、「受信機／デコーダを介して送信機からコンピュータにコンピュータファイルのダウンロード（代理人参照番号ＰＣ／ＡＳＢ／１９７１１）」、「テレビジョンプログラムおよび他のデータの送信および受信（代理人参照番号ＰＣ／ＡＳＢ／１９７１２）」、「データのダウンロード（代理人参照番号ＰＣ／ＡＳＢ／１９７１３）」、「コンピュータメモリ構成（代理人参照番号ＰＣ／ＡＳＢ／１９７１４）」、「テレビジョンあるいはラジオ制御システム生成（代理人参照番号ＰＣ／ＡＳＢ／１９７１５）」、「送信データストリームからのデータセクシ

ョンの抽出（代理人参照番号ＰＣ／ＡＳＢ／１９７１６）」、「アクセス制御システム（代理人参照番号ＰＣ／ＡＳＢ／１９７１７）」、「データ処理システム（代理人参照番号ＰＣ／ＡＳＢ／１９７１８）」、および「放送・受信システム、およびそのための受信機／デコーダおよび遠隔コントローラ（代理人参照番号ＰＣ

／ＡＳＢ／１９７２０）」である。これらの文書の開示は参照してここに組み込まれている。出願のリストは本出願を含んでいる。

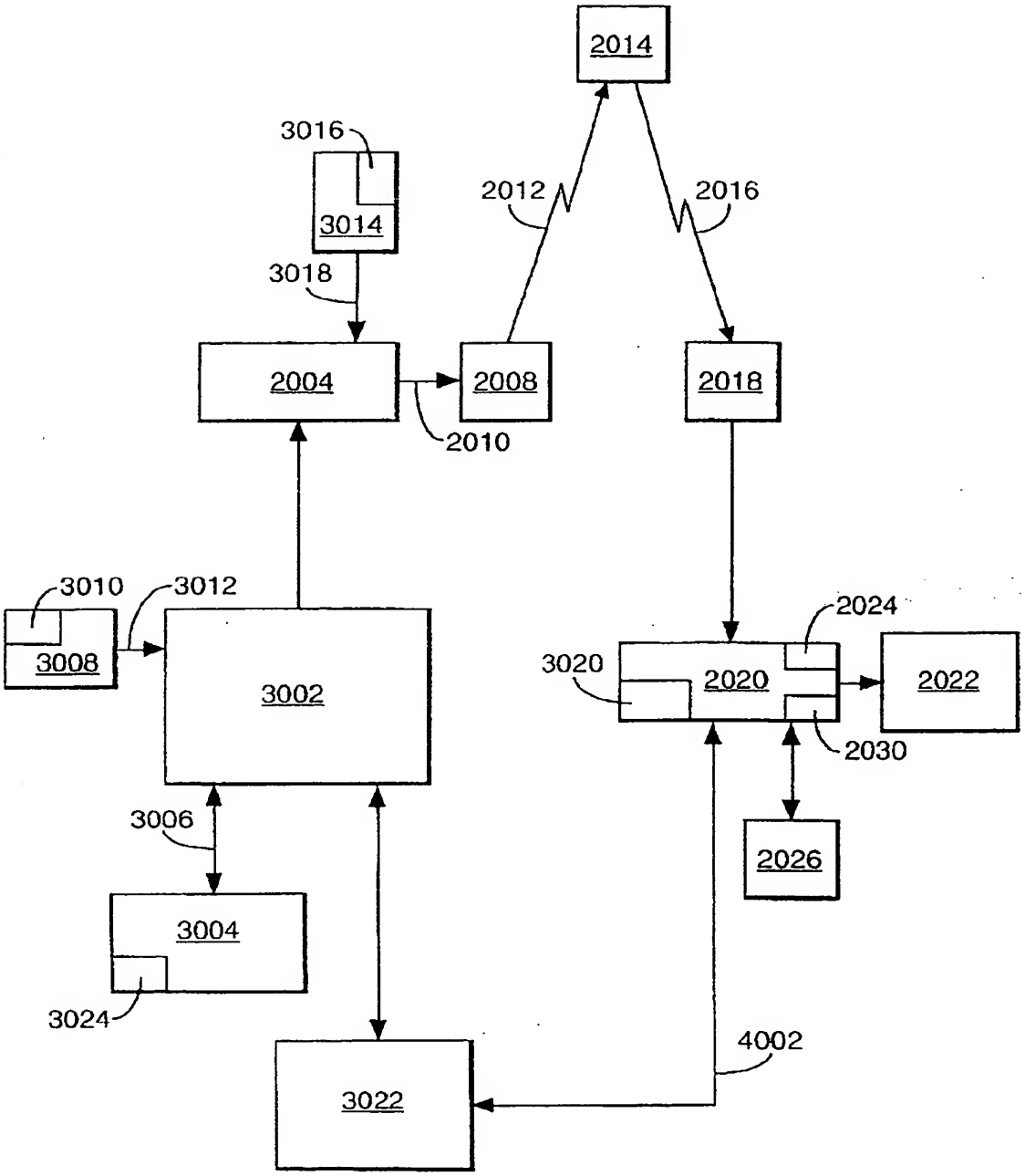
【図１】

Fig.1.


2000
2014
2012
2016
2006
2010
2002
2004
2008
2018
4000
2020
2022
4000
3000
4002
3000
1000

【図２】

Fig.2.


2014
3016
3014
2012
2016
3018
2004
2008
2018
2010
3010
3012
3008
3002
2024
3020
2020
2022
2030
3006
2026
3004
3024
4002
3022

【図３】

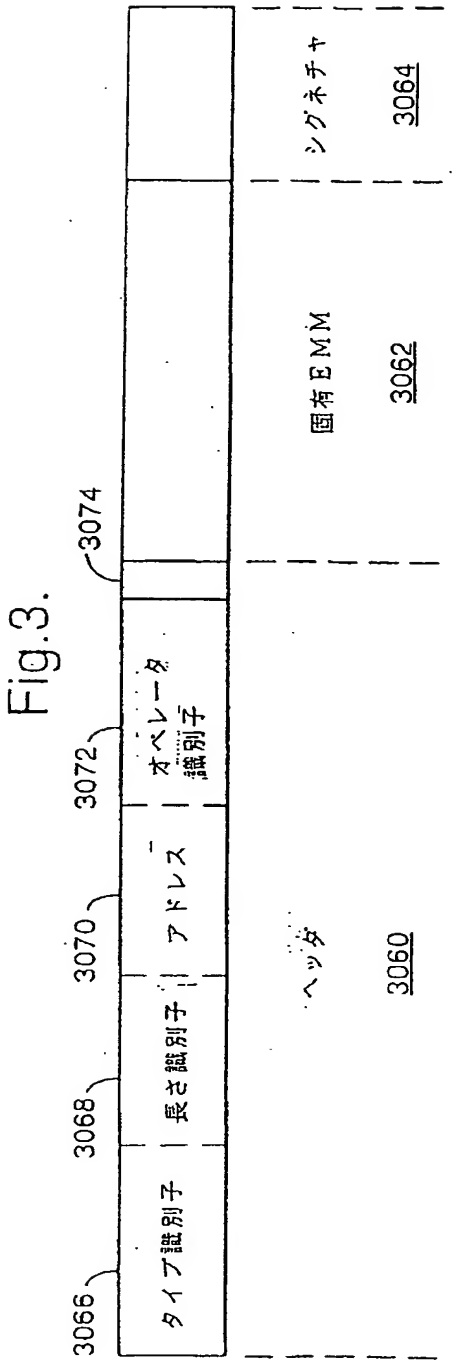


Fig.3.
3066
タイプ識別子
3068
長さ識別子
3070
アドレス
3072
オペレータ識別子
3074
ヘッダ
3060
固有ＥＭＭ
3062
シグネチャ
3064

【図４】

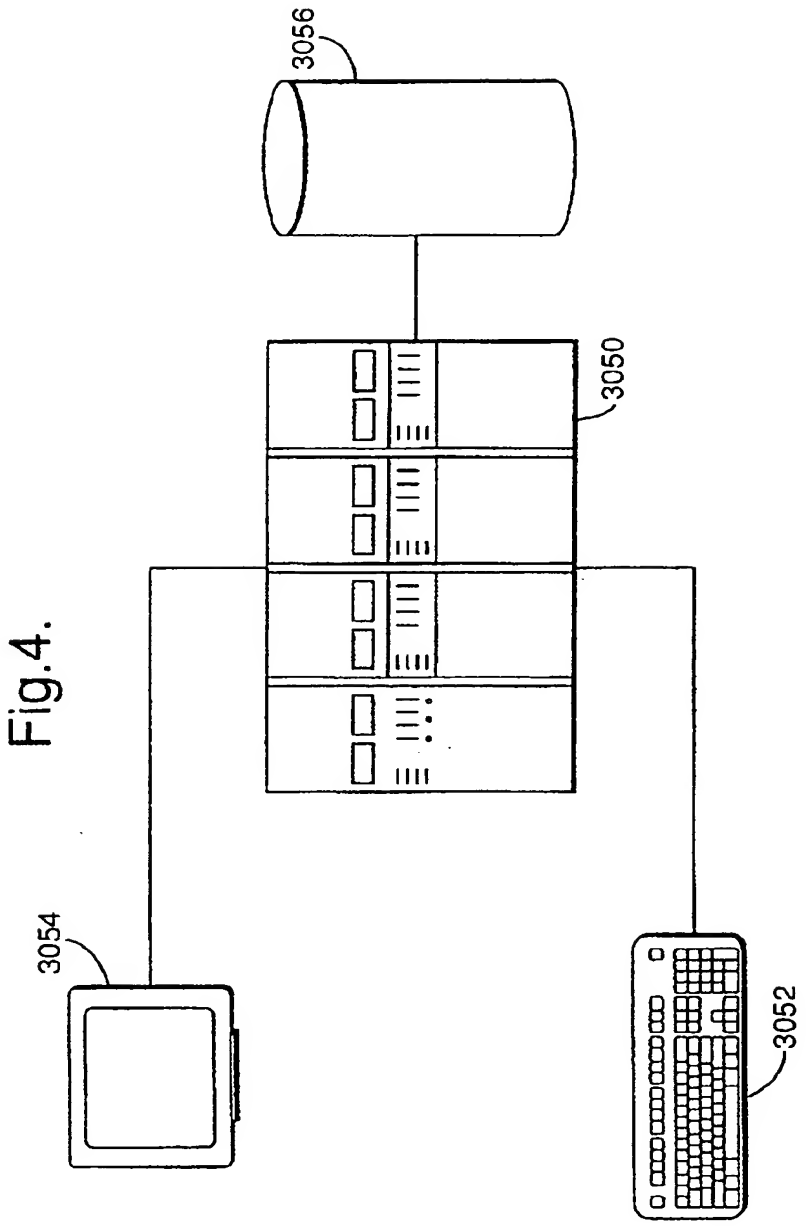
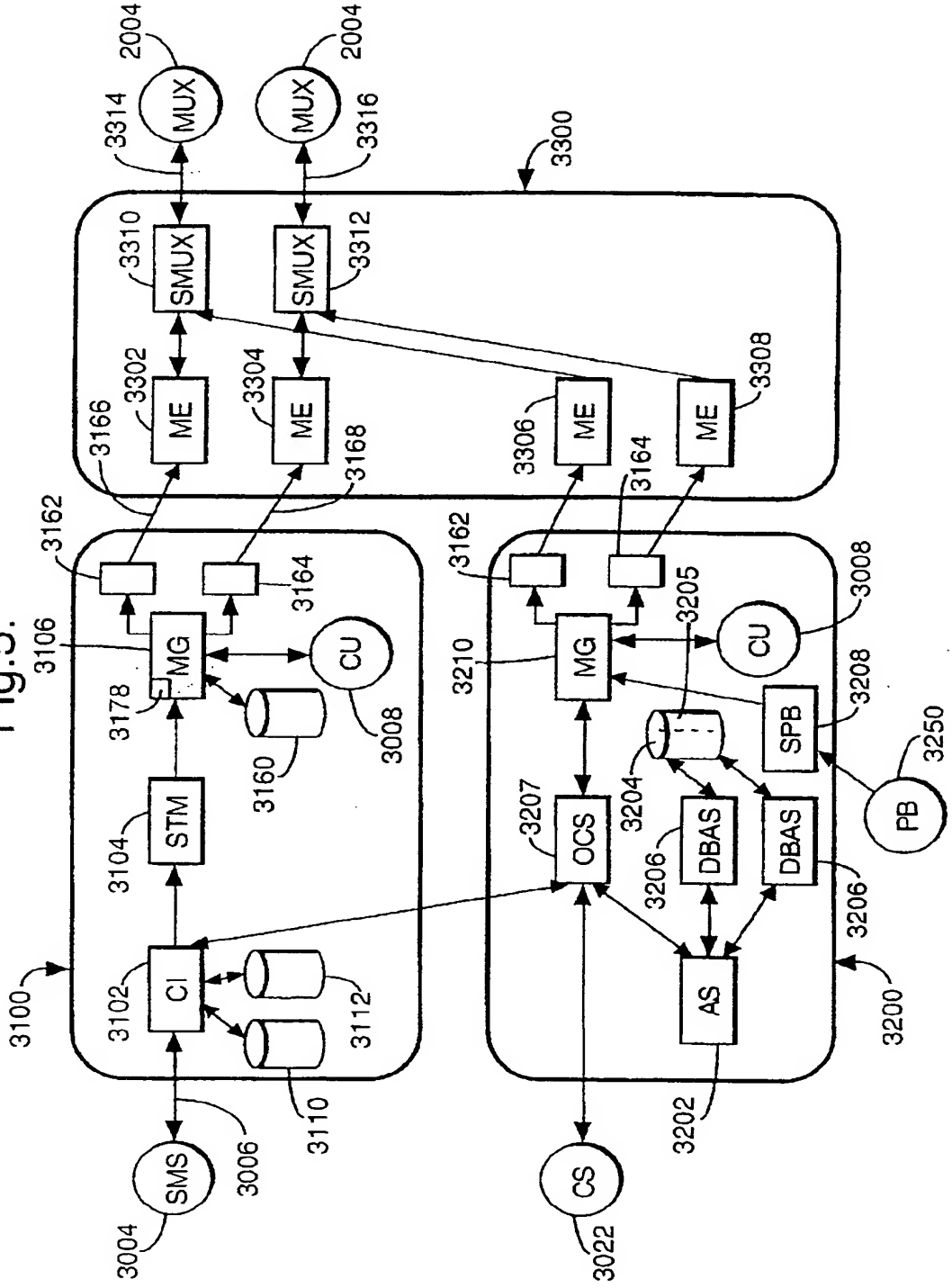


Fig.4.

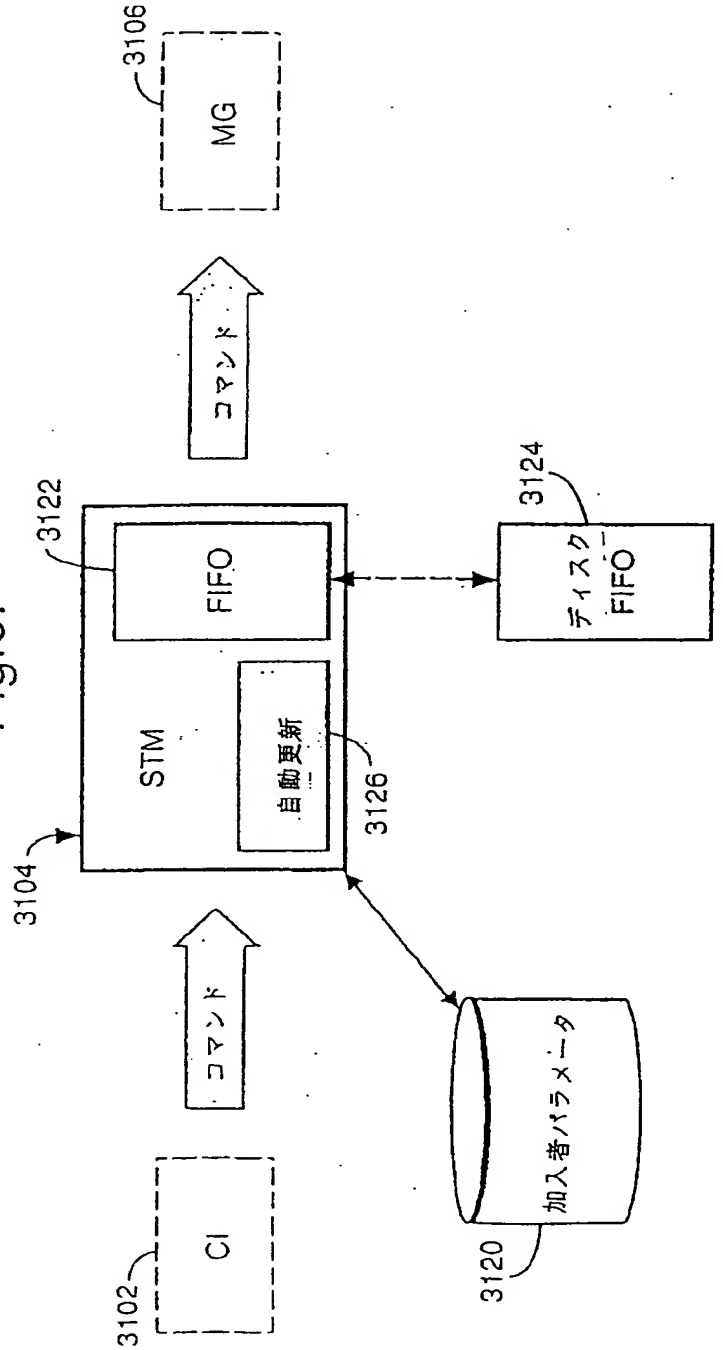
【図５】

Fig.5.


2004
MUX
3314
3316
3300
SMUX
3310
3312
3302
3304
3306
3308
ME
3166
3168
3164
3162
3106
MG
3178
CU
3008
3160
3104
STM
3102
CI
3112
3110
3100
SMS
3006
3004
3205
3210
3207
OCS
3204
DBAS
3206
SPB
PB
3250
AS
3202
CS
3022
3200

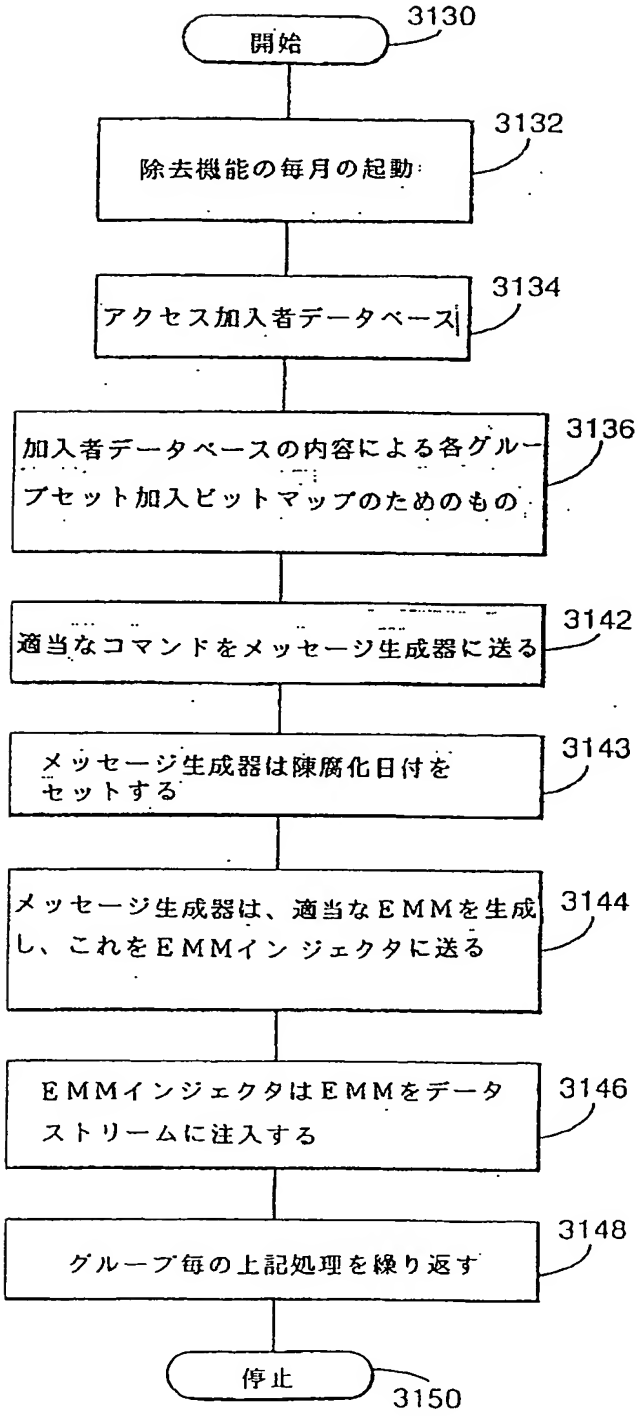
【図６】

Fig.6.


3106
MG
コマンド
3122
FIFO
3124
ディスク FIFO
STM
自動更新
3126
3104
コマンド
加入者パラメータ
CI
3102
3120

【図７】

Fig.7.


開始
3130
除去機能の毎月の起動
3132
アクセス加入者データベース
3134
加入者データベースの内容による各グループセット加入ビットマップのためのもの
3136
適当なコマンドをメッセージ生成器に送る
3142
メッセージ生成器は陳腐化日付をセットする
3143
メッセージ生成器は、適当なＥＭＭを生成し、これをＥＭＭインジェクタに送る
3144
ＥＭＭインジェクタはＥＭＭをデータストリームに注入する
3146
グループ毎の上記処理を繰り返す
3148
停止
3150

【図８】

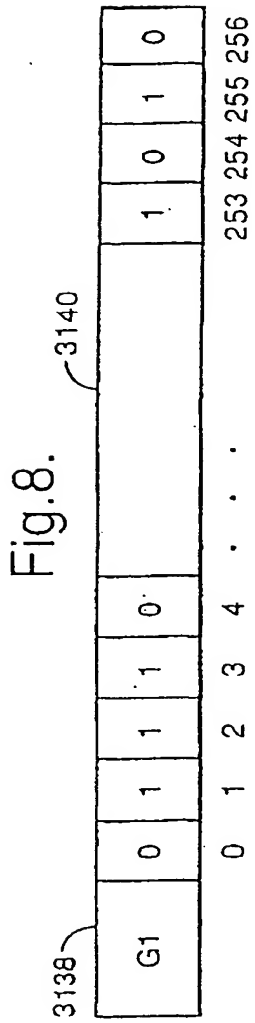


Fig.8.

【図９】

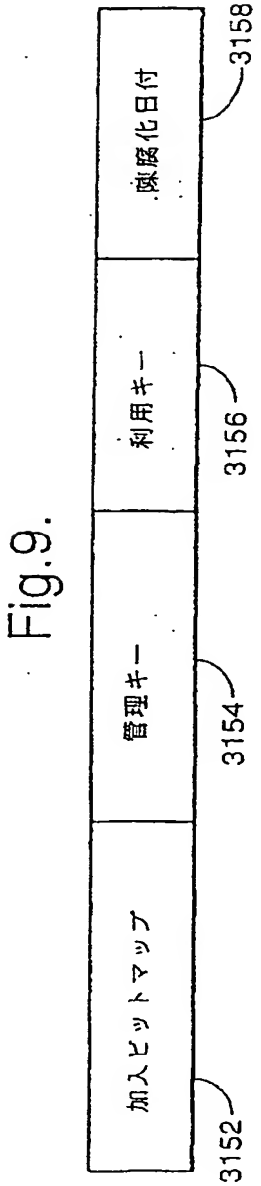
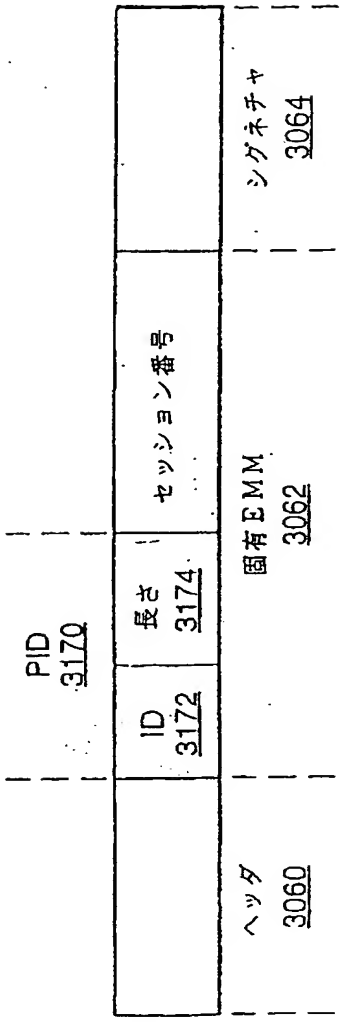


Fig.9.

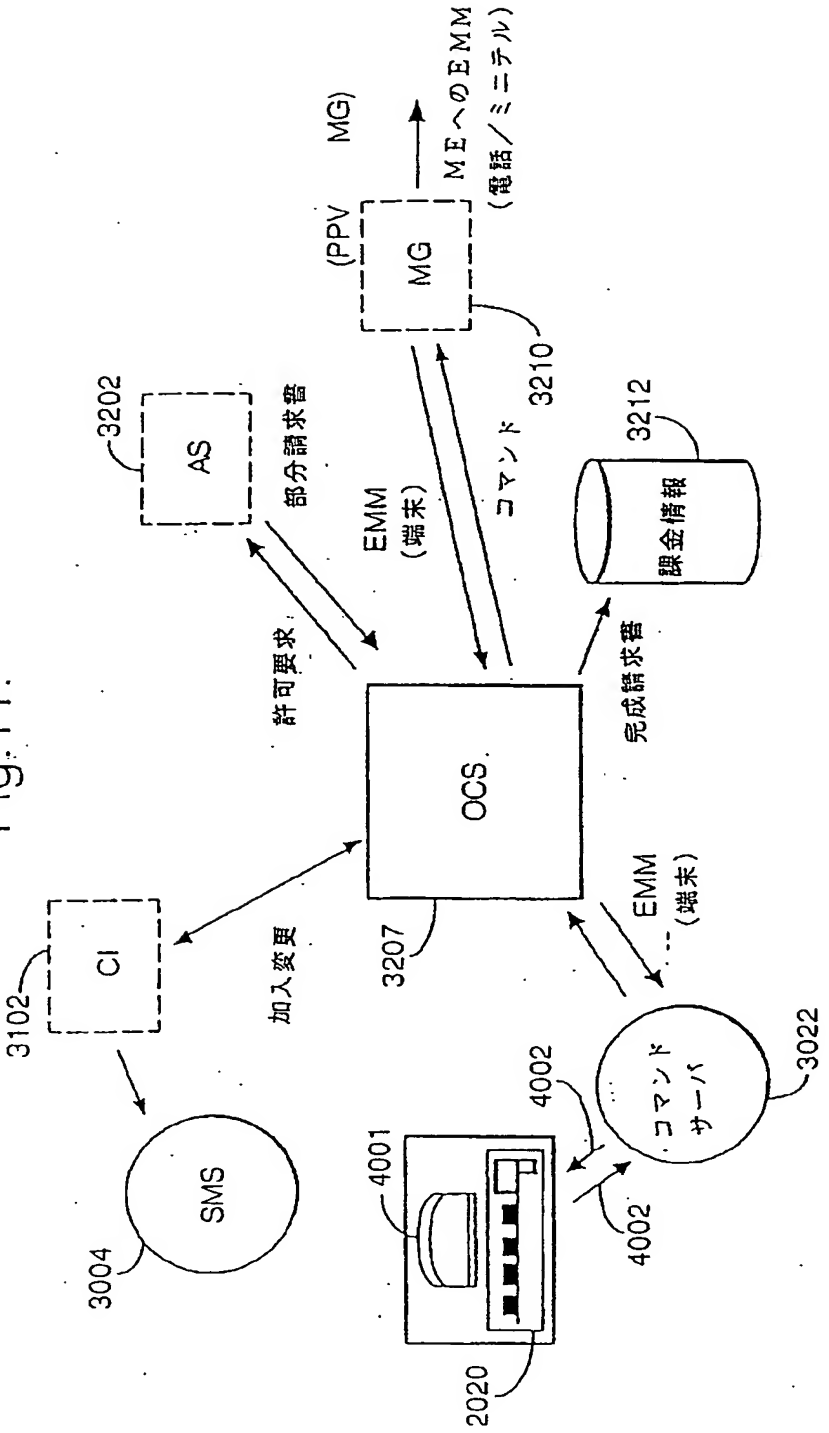
【図１０】

Fig.10.


ヘッダ
3060
PID
3170
ID
3172
長さ
3174
セッション番号
固有ＥＭＭ
3062
シグネチャ
3064

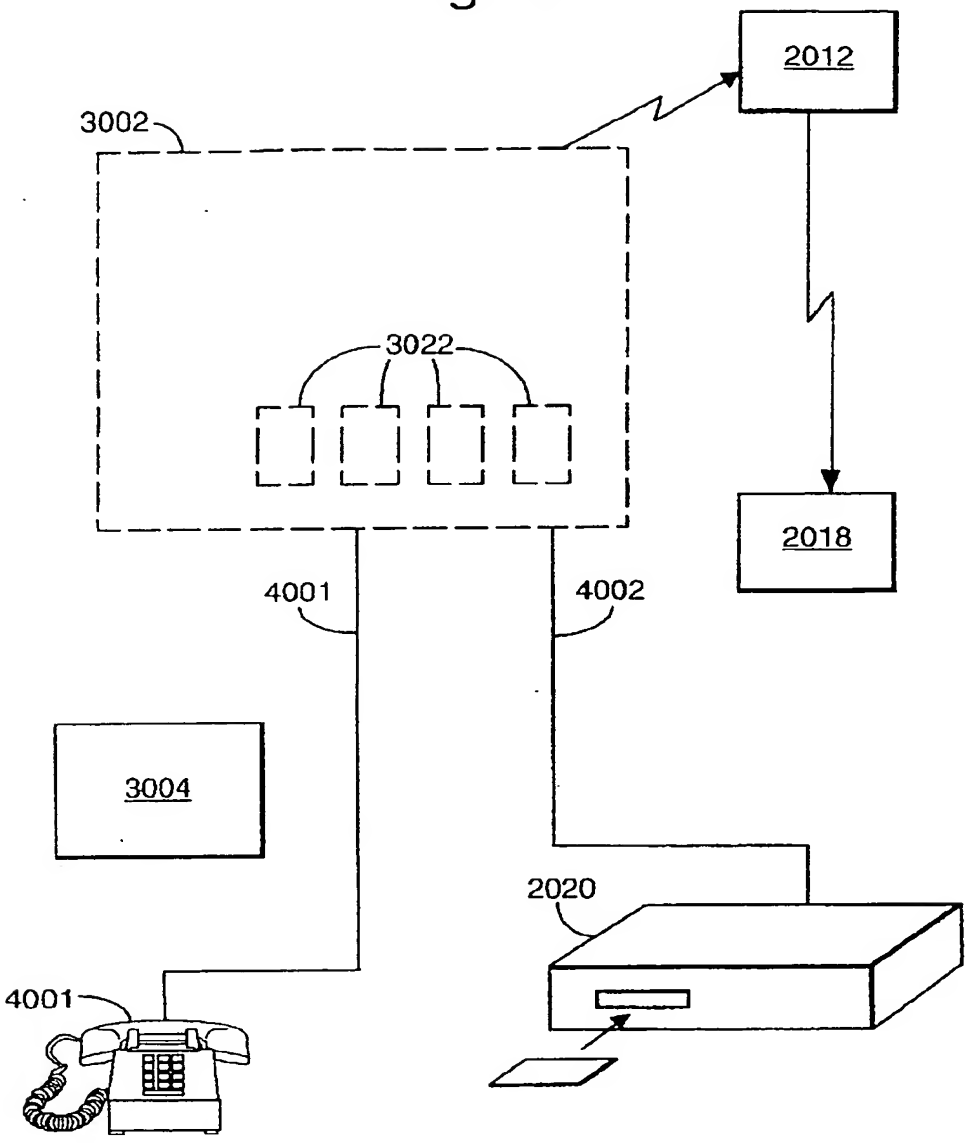
【図１１】

Fig.11.


(PPV MG)
MEへのEMM
(電話／ミニテル)
MG
3210
3202
AS
部分請求書
EMM
(端末)
コマンド
3212
課金情報
許可要求
OCS
完成請求書
CI
3102
加入変更
3207
EMM
(端末)
SMS
3004
4001
4002
コマンド
サーバ
3022
4002
2020

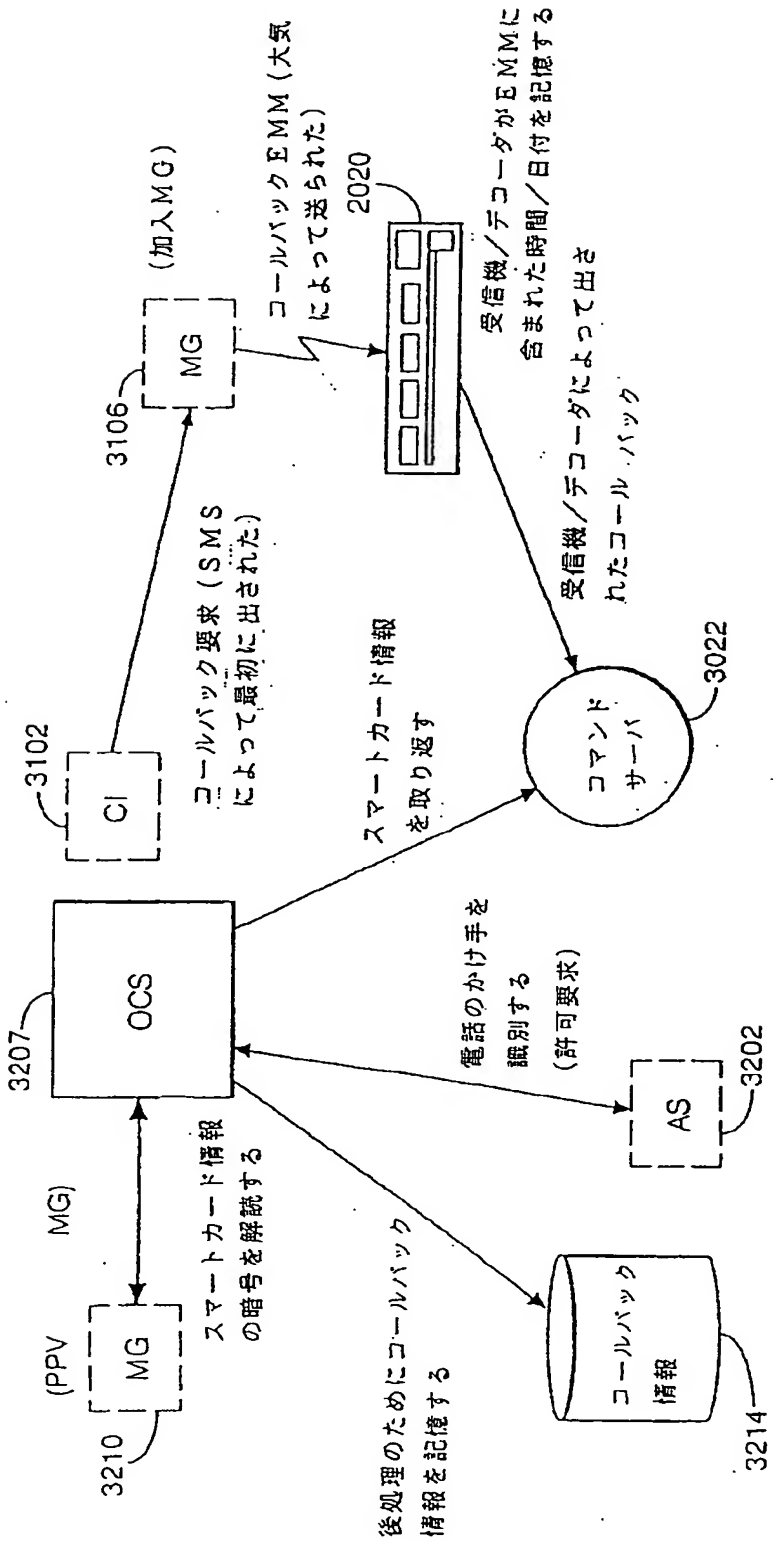
【図１２】

Fig.12.



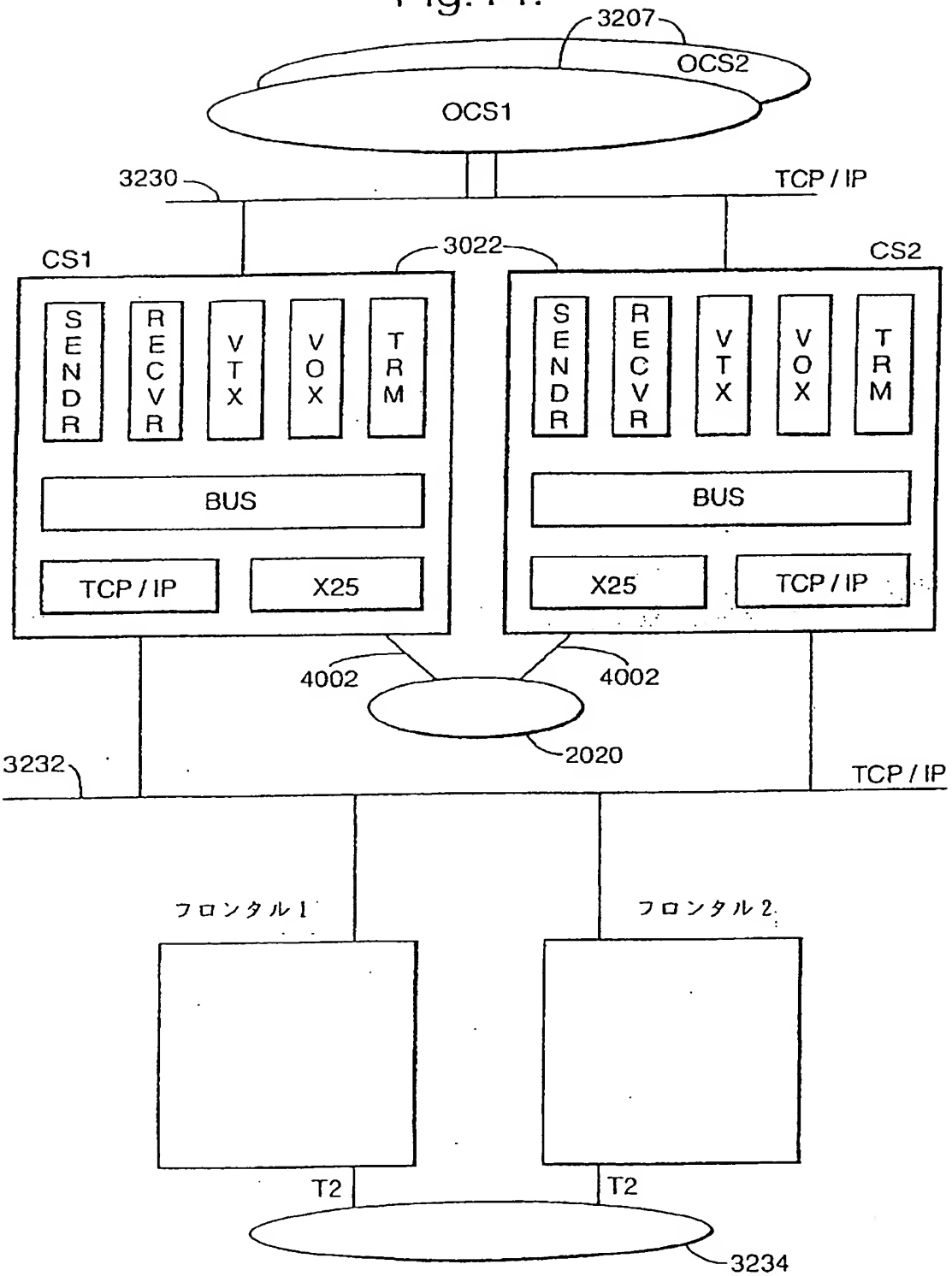
【図１３】

Fig.13.


3102
CI
3106
MG
(加入MG)
コールバック要求（SMS
によって最初に出された）
コールバックEMM（大気
によって送られた）
2020
受信機／デコーダがEMMに
含まれた時間／日付を記憶する
受信機／デコーダによって出さ
れたコールバック
スマートカード情報
を取り返す
コマンド
サーバ
3022
3207
OCS
電話のかけ手を
識別する
（許可要求）
AS
3202
(PPV
MG)
スマートカード情報
の暗号を解読する
後処理のためにコールバック
情報を記憶する
コールバック
情報
3214
3210
MG

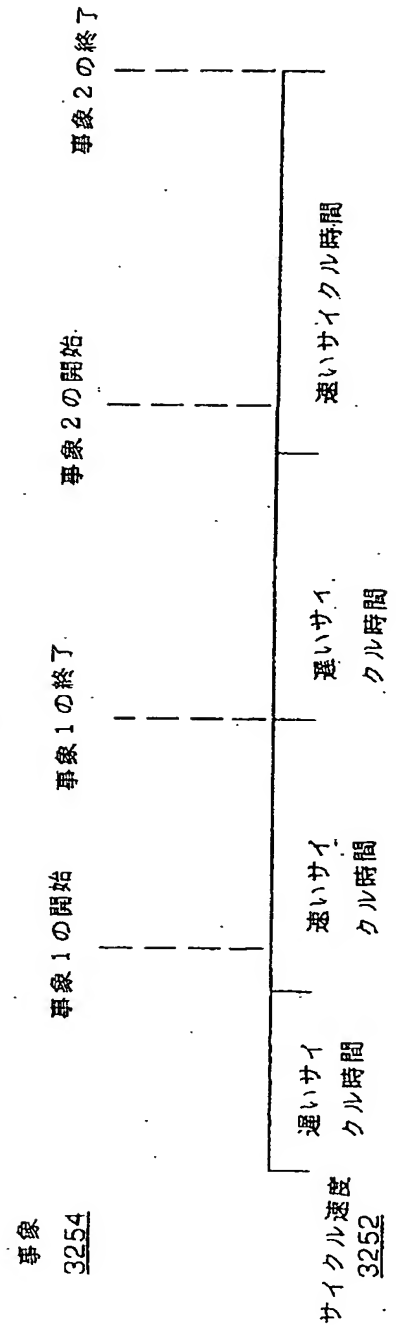
【図１４】

Fig.14.


3207
OCS2
OCS1
3230
TCP / IP
CS1
3022
CS2
SENDR
RECVR
VTX
VOX
TRM
BUS
TCP / IP
X25
4002
4002
2020
3232
TCP / IP
フロンタル１
フロンタル２
T2
T2
3234

【図１５】

Fig.15.


事象
3254
サイクル速度
3252
事象１の開始
事象１の終了
事象２の開始
事象２の終了
遅いサイクル時間
遅いサイクル時間
遅いサイクル時間
遅いサイクル時間

【図１６】

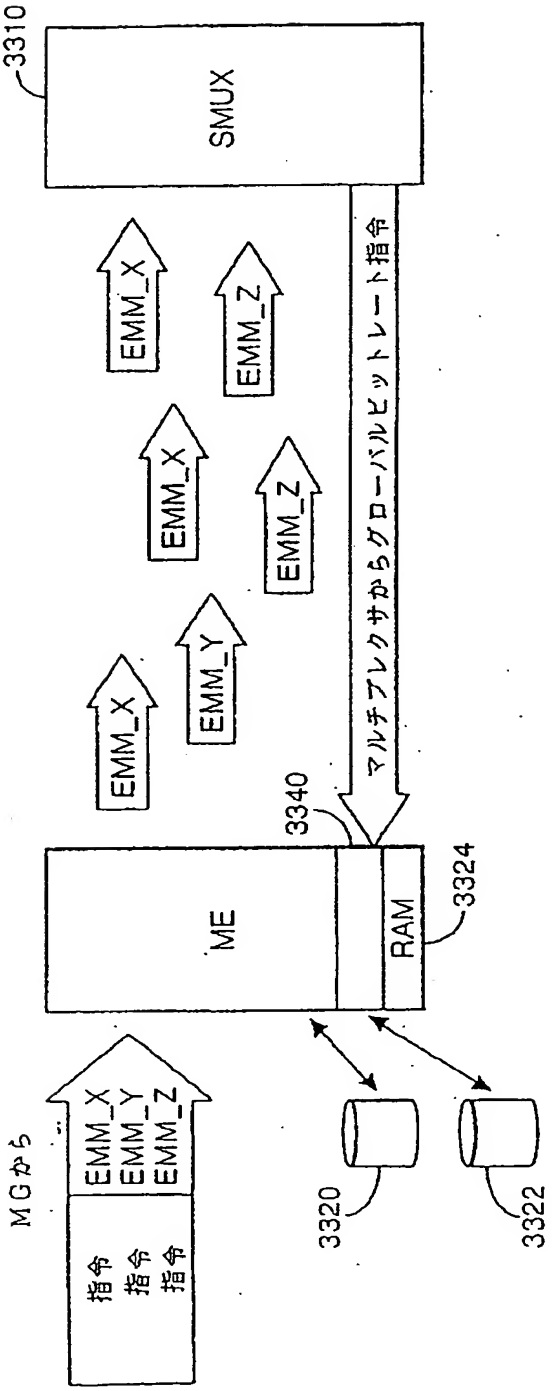
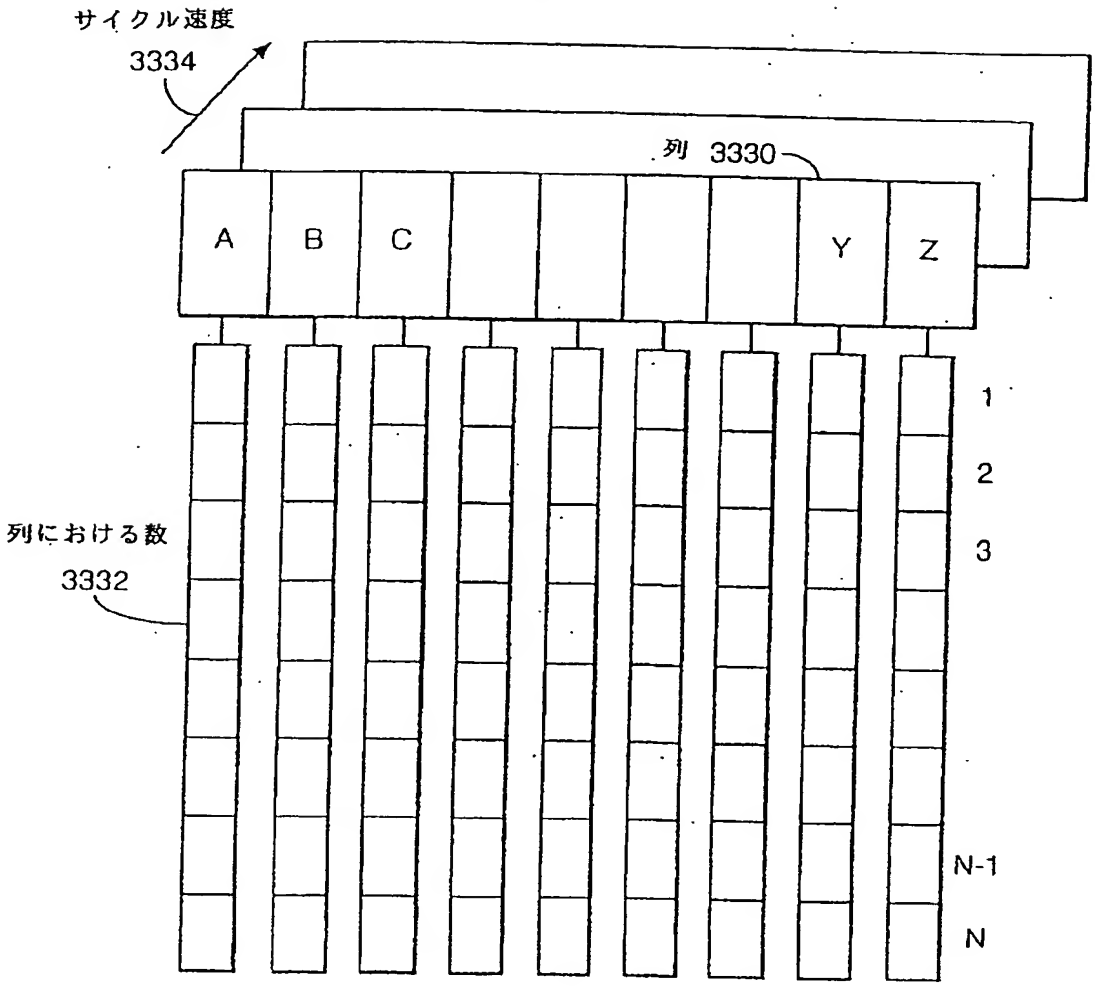

3310
SMUX
マルチプレクサからクローバルビットレート指令
EMM_X
EMM_Z
EMM_X
EMM_Z
EMM_Y
EMM_X
3340
ME
RAM
3324
MGから
EMM_X
EMM_Y
EMM_Z
指令
指令
指令
3320
3322

Fig.16.

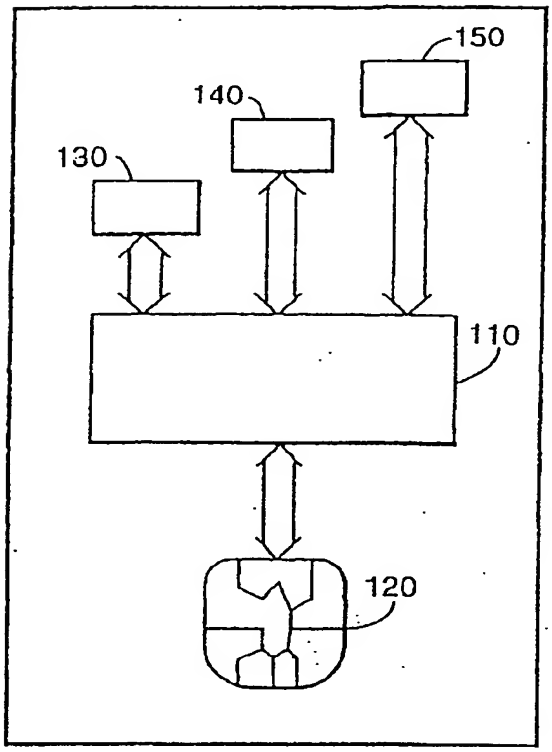
【図１７】

Fig.17.



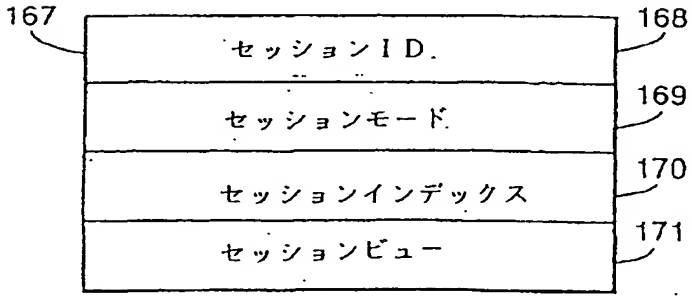
【図１８】

Fig.18.



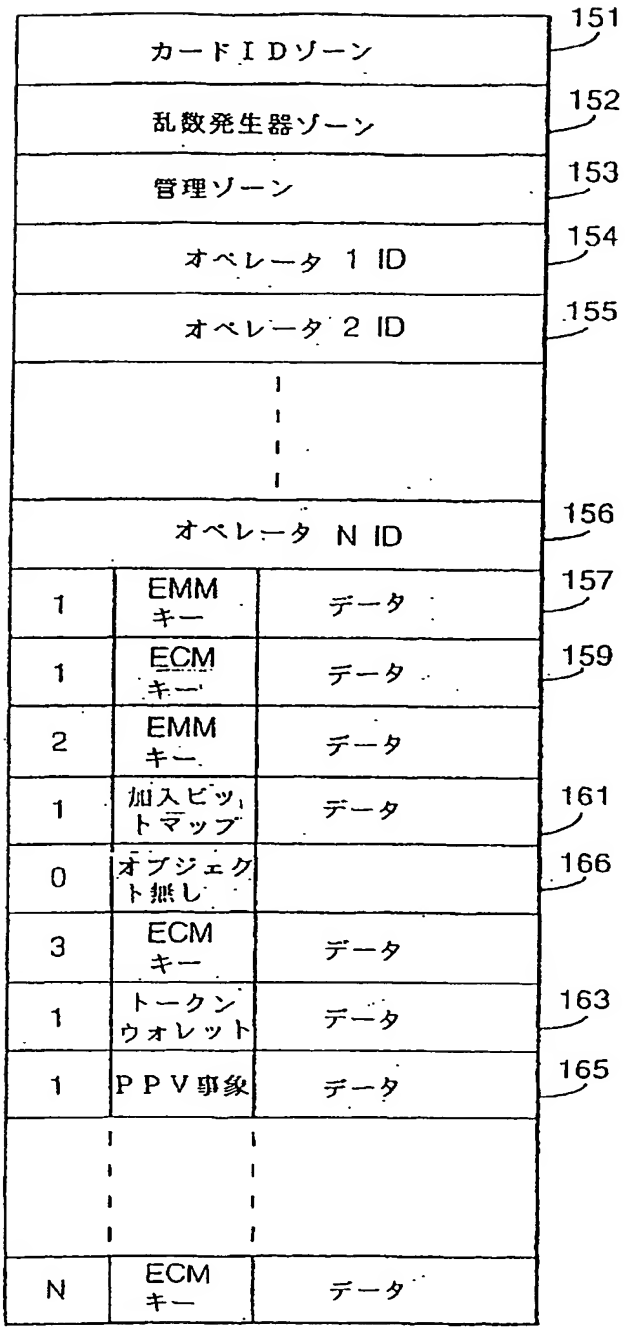
【図２０】

Fig.20.



【図１９】

Fig.19.


カードＩＤゾーン
151
乱数発生器ゾーン
152
管理ゾーン
153
オペレータ １ ID
154
オペレータ ２ ID
155
オペレータ Ｎ ID
156
1 EMM キー データ
157
1 ECM キー データ
159
2 EMM キー データ
1 加入ビットマップ データ
161
0 オブジェクト無し
166
3 ECM キー データ
1 トークンウォレット データ
163
1 ＰＰＶ事象 データ
165
N ECM キー データ

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/EP 97/02107

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N7/16 H04N7/167

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 144 663 A (KUDELSKI ANDRE ET AL) 1 September 1992 see column 4, line 58 - line 63 see column 5, line 62 - column 6, line 61 see column 8, line 48 - line 58 see figures 1-4,8-11	1-14, 36-47
X	WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ;CHANEY JOHN WILLIAM (US)) 29 February 1996 see page 1, line 21 - page 3, line 11 see page 6, line 1 - page 23, line 20 see figures 1-8	1-8, 11-14, 25-29, 40-47

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publicationdate of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theInternational search	Date of mailing of the international search report
12 November 1997	24/11/1997

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter... onal Application No
PCT/EP 97/02107

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TASKETT J: "SMART CARDS AS A REPLACEABLE SECURITY ELEMENT FOR TELEVISION DELIVERY ACCESS CONTROL" PROCEEDINGS FROM ELEVEN TECHNICAL SESSIONS OF THE ANNUAL CONVENTION AND EXPOSITION OF THE NATIONAL CABLE TELEVISION ASSOCIATION, SAN FRANCISCO, JUNE 6 - 9, 1993, no. CONVENTION 42, 6 June 1993, RUTKOWSKI K, pages 128-132, XP000410492 see the whole document	1-14, 36-47
X	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 see page 8, line 44 - page 11, line 23 see page 12, line 46 - page 15, line 3 see figures 4,5,7-10 see figures 12,13	15-20, 22,24-49
A	VIGARIE J P: "A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER" CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 June 1993, POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP000379391 see the whole document	15-50

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter ional Application No
PCT/EP 97/02107

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5144663 A	01-09-92	AU 599646 B	26-07-90
		AU 7157887 A	22-10-87
		DE 3751410 D	24-08-95
		DE 3751410 T	11-04-96
		EP 0243312 A	28-10-87
		EP 0626793 A	30-11-94
		ES 2076931 T	16-11-95
		JP 2610260 B	14-05-97
		JP 63023488 A	30-01-88
		JP 2520217 B	31-07-96
		JP 5244591 A	21-09-93
WO 9606504 A	29-02-96	AU 3238595 A	22-03-96
		AU 3239495 A	14-03-96
		CA 2196406 A	07-03-96
		CA 2196407 A	29-02-96
		EP 0782807 A	09-07-97
		FI 970677 A	18-02-97
		PL 318647 A	07-07-97
		WO 9607267 A	07-03-96
EP 0679029 A	25-10-95	US 5237610 A	17-08-93
		EP 0683614 A	22-11-95
		AT 144670 T	15-11-96
		AU 650958 B	07-07-94
		AU 1384092 A	01-10-92
		CN 1066950 A,B	09-12-92
		DE 69214698 D	28-11-96
		DE 69214698 T	06-03-97
		EP 0506435 A	30-09-92
		JP 5145923 A	11-06-93

フロントページの続き

(51)Int.Cl.'		識別記号	F I			テーマコード (参考)
G09C	1/00	660	G06K	19/00	N	
H04H	1/00				Q	
H04L	9/10		H04L	9/00	621A	

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(GH, KE, LS, MW, SD, SZ, UG), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU